RAPPORT ANNUEL 2018

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

INTRODUCTION

La Commission nationale pour la protection des données (CNPD) est un établissement public indépendant doté de la personnalité juridique. Elle jouit de l'autonomie financière et administrative.

Elle est chargée de vérifier la légalité des fichiers et de toutes collectes, utilisations et transmissions de renseignements concernant des individus identifiables et doit assurer dans ce contexte le respect des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée.

Elle doit notamment contrôler et vérifier si les données soumises à un traitement sont traitées en conformité avec les dispositions :

- du règlement général sur la protection des données ;
- de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données ;
- de la loi du 1er août 2018 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 ;
- de la loi modifiée du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques ;
- des textes légaux prévoyant des dispositions spécifiques en matière de protection des données à caractère personnel.

Elle n'est pas compétente pour contrôler les opérations de traitement de données à caractère personnel 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. Cette mission revient à l'autorité de contrôle de la protection des données judiciaires.

INTRODUCTION

MISSIONS

Informer et guider avec :
- La sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement ;
- La sensibilisation des responsables du traitement et des sous-traitants en ce qui concerne les obligations qui leur incombent.

Conseiller 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 évolutions pertinentes, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et de la communication et des pratiques commerciales ;
- La promotion des bonnes pratiques et la publication de lignes d'orientations thématiques ;
- L'approbation de codes de conduite, des schémas de certification et l'agrément des organismes de certification ;
- Les recommandations au responsable du traitement conformément à la procédure de consultation préalable.

Superviser et assurer la transparence par :
- Les contrôles suite à des réclamations ou de sa propre initiative ;
- Les audits sur la protection des données ;
- L'intervention suite à des violations de données ;
- La tenue à jour des registres internes des violations au RGPD ;
- L'établissement et la tenue à jour d'une liste en lien avec l'obligation d'effectuer une analyse d'impact relative à la protection des données ;
- L'approbation des règles d'entreprise contraignantes ;
- L'examen des certifications et la surveillance des certificateurs;
- L'adoption de mesures correctrices (p.ex. avertissement, interdiction d'un traitement ou amende administrative).

Coopérer à travers :
- Les échanges avec d'autres autorités de contrôle nationales ou étrangères ;
- La contribution aux activités du Comité européen de la protection des données.

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. Elle promeut une atmosphère positive et ouverte.

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

TABLE DES MATIÈRES

1 AVANT-PROPOS 8

2 L'ANNÉE 2018 EN UN COUP D'ŒIL 12

3 LES ACTIVITÉS EN 2018 16

1 SENSIBILISATION, GUIDANCE ET CONSEIL 16

1.1 Actions de sensibilisation 16
1.2 Organisation de formations et conférences 21
1.3 Elaboration de guidances 26
1.4 Avis et recommandations 29
1.5 Traitement des demandes de renseignements 39

2 CONFORMITÉ ET CONTRÔLE 41

2.1 Traitements des réclamations 41
2.2 Contrôles effectués 44
2.3 Notification des violations de données 46
2.4 Désignation des délégués à la protection des données 53
2.5 Consultation préalable dans le cadre d'une analyse d'impact relative à la protection des données 54
2.6 Certifications 56
2.7 Transferts internationaux de données personnelles 57
2.8 Mesures correctrices et sanctions 60
2.9 Traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale 62
2.10 Rétention de données de trafic et de localisation 62

3 TRAVAIL AU NIVEAU INTERNATIONAL 63
3.1 Le Comité Européen de la Protection des Données 63
3.2 Le « Groupe de Berlin » 68
3.3 Conférence de printemps des autorités européennes à la protection des données 69
3.4 Conférence internationale des commissaires de la protection des données 69
3.5 Le séminaire européen « Case Handling Workshop » 70
3.6 Signature du protocole d'amendement de la Convention 108 du Conseil de l'Europe 70

4 RESSOURCES, STRUCTURES ET FONCTIONNEMENT 72
1 RAPPORT DE GESTION RELATIF AUX COMPTES DE L'EXERCICE 2018 72

2 PERSONNEL ET SERVICES 77

3 ORGANIGRAMME DE LA CNPD 78
3.1 Organigramme du 01.01.2018 au 24.05.2018 78
3.2 Organigramme du 25.05.2018 au 31.12.2018 79

5 ANNEXES 80

AVANT-PROPOS

1

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

Depuis le 25 mai 2018, le règlement général sur la protection des données[1] ou « RGPD » est applicable. Ce nouveau cadre légal a vocation à établir un cadre harmonisé au sein de l'Union européenne et remplace la directive de 1995[2]. Le règlement européen a été complété au niveau national par la loi du 1er août 2018 portant organisation de la CNPD et du régime général sur la protection des données. La loi du 1er août 2018 relative à la protection des données en matière pénale ainsi qu'en matière de sécurité nationale quant à elle a transposé la Directive (UE) 2016/680[3].

Les formalités préalables (notifications et autorisations) que les organismes devaient introduire auprès de la CNPD pour certains traitements ont été supprimées – ceci afin de se conformer à la nouvelle philosophie du RGPD visant à responsabiliser davantage les acteurs qui traitent des données personnelles.

En raison de cette nouvelle approche dite d'« accountability », la CNPD est passée d'un système de contrôle a priori vers un contrôle a posteriori. Ce changement de paradigme lui permet de se concentrer davantage sur ses missions de sensibilisation du grand public, de guidance des responsables du traitement et d'enquête.

La CNPD se prépare depuis quelques années activement à ce nouveau régime et en 2018, elle a continué son approche générale, qui consiste à assurer un équilibre entre guidance et contrôle.

[1] 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

[2] Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[3] 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

UNE COMMISSION TRÈS SOLLICITÉE

L'entrée en application des nouvelles règles a été accompagnée par une prise de conscience inédite des enjeux de protection des données auprès des professionnels et des particuliers. Cela a conduit à une augmentation importante des sollicitations de la CNPD.

Ainsi, la CNPD a reçu 1.112 demandes de renseignement par écrit en 2018, soit plus que le double qu'en 2017 où elle en avait reçu 528. Ce nombre élevé s'explique par l'effet médiatique du RGPD et des acteurs de plus en plus sensibilisés.

De nombreuses questions ont porté sur la mise en conformité à la nouvelle législation. D'autres demandes récurrentes concernaient notamment la vidéosurveillance (du domicile privé et sur le lieu de travail), le délégué à la protection des données ou encore le droit d'accès et les autres droits des personnes concernées (droit à l'effacement, droit d'opposition, droit de rectification, etc.).

La Commission nationale a, par ailleurs, participé au processus législatif avec 27 avis (soit 5 de plus qu'en 2017) 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 place du dossier de soins partagé, la lutte contre le blanchiment et contre le financement du terrorisme, la réorganisation du Service de renseignement de l'État, RENITA (réseau national intégré de radiocommunication pour les services de sécurité et de secours luxembourgeois), la modernisation du droit de la faillite, le registre des bénéficiaires effectifs ou encore les sanctions administratives communales.

VERS PLUS DE GUIDANCE ET DE SENSIBILISATION

A l'occasion de l'entrée en application du nouveau règlement, la CNPD a lancé sa campagne de sensibilisation « Vos données? Vos droits! ». Du 25 mai au 11 juin, l'autorité de protection des données a organisé plusieurs événements, a distribué 12.000 brochures et gadgets dans de nombreux endroits stratégiques du Grand-Duché et est intervenue dans les médias.

Le 4 juin, la CNPD a réuni de prestigieux orateurs afin de célébrer 4 décennies de protection des données à la Rockhal. Le premier Ministre, Monsieur Xavier Bettel, la Commissaire européenne à la justice, aux consommateurs et à l'égalité des genres, Madame Vera Jourova, et la présidente du Comité Européen de la Protection des Données, Madame Andre Jelinek, y sont notamment intervenus.

La CNPD a mis l'accent sur de nombreuses mesures de sensibilisation et de guidance en 2018, dont notamment :

- la création de sa nouvelle brochure à l'attention du grand public dont le but est de présenter les droits des citoyens en matière de protection des données et d'expliquer comment les faire valoir ;
- l'élaboration de nouvelles lignes directrices en matière de vidéosurveillance, concernant le droit à l'image, relatives aux règles de protection des données dans le cadre des élections sociales et pour le monde associatif ;

- la publication de plusieurs formulaires (notification de violations de données, déclaration du délégué à la protection des données, demande de consultation préalable) facilitant la tâche aux responsables du traitement ;
- la formation de plus de 500 personnes lors de 12 sessions d'introduction à la protection des données;
- l'organisation du premier « DaProLab (CNPD's Open Data Protection Laboratory) » sur l'évaluation des impacts sur les personnes concernées d'une violation de données dans le milieu hospitalier, des cabinets médicaux et laboratoires médicaux ;
- l'organisation de workshops s'adressant principalement aux utilisateurs du « GDPR Compliance Support Tool », un outil leur permettant de vérifier le niveau de maturité de leur organisation en matière de protection des données ; ou encore
- la participation à plus de 86 conférences et formations à l'attention de publics plus spécialisées (Chambre de Commerce, Chambre des Métiers, ABBL, Université du Luxembourg, etc.).

UN NOMBRE RECORD DE RÉCLAMATIONS

Le nombre de réclamations de personnes qui ont estimé qu'il y a eu une violation de la loi ou une entrave à l'exercice de leurs droits a plus que doublé par rapport à l'année précédente, de 200 en 2017 à 450 en 2018. Le RGPD a eu un impact important: lors des 5 premiers mois de l'année, la CNPD a reçu en moyenne 18 plaintes par mois, tandis que pour les 7 prochains mois, elle en a reçu 51 par mois.

Presqu'un quart des plaintes (24%) était motivé par le non-respect du droit d'accès par les responsables du traitement. Les demandes d'effacement ou de rectification de données auxquelles les suites souhaitées n'avaient pas été réservées ont constitué 16% des plaintes. Dans 15% des cas, les plaignants ont demandé à la CNPD de vérifier la licéité de certaines pratiques administratives ou commerciales. Ils ont notamment remis en cause les conditions générales relatives à des commerces ou des services en ligne ou encore la durée de conservation des données collectées.

RENFORCEMENT DE LA MÉTHODOLOGIE D'ENQUÊTE : AUDITS ET CONTRÔLES SUR PLACE

La CNPD a adapté sa stratégie et mis en place des enquêtes dites « proactives ». Ces enquêtes sont effectuées sous la forme d'audits thématiques portant sur les nouvelles obligations du RGPD.

Vu l'impact du nouveau rôle du délégué à la protection des données (DPD) et l'importance de son intégration dans l'entreprise, la CNPD a décidé de lancer une campagne d'enquête thématique sur la fonction du DPD. Ainsi, 25 procédures d'audit ont été ouvertes en 2018.

La CNPD a également réalisé des contrôles réactifs sur base d'incidents, de réclamations, d'informations relayées dans les médias ou faisant suite à un contrôle précédent. 12 enquêtes sur place ont eu lieu en 2018 dans les domaines de la vidéosurveillance, de la géolocalisation, de la publicité et du marketing.

Le siège de la CNPD à Belval

CAUSE PRINCIPALE DES VIOLATIONS DE DONNÉES : L'ERREUR HUMAINE

Depuis le 25 mai 2018, les responsables de traitement doivent notifier les violations de données à caractère personnel à la CNPD dans un délai de 72 heures après en avoir pris connaissance si la violation en question est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. En 2018, 172 violations de données ont été notifiées à la CNPD. La principale cause de violation de données à caractère personnel est l'erreur humaine.

Pour y remédier, les entreprises doivent donc renforcer le facteur humain. Cela passe avant tout par la sensibilisation et la formation du personnel qui doit être systématique et régulière.

PERSPECTIVES D'AVENIR

Après l'entrée en application du RGPD, la CNPD consolide ses nouvelles structures et procédures. En 2019, elle poursuivra ses efforts d'accompagnement des acteurs dans l'application conforme de la législation en matière de protection des données personnelles et renforcera le contrôle du respect des obligations en découlant en coopération avec ses homologues européens.

Luxembourg, le 16 mai 2019

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire

L'ANNÉE 2018 EN UN COUP D'ŒIL

2

JANVIER

28 • 12e Journée de la protection des données

28 • La CNPD publie sa nouvelle brochure de sensibilisation du grand public « Vos données ? Vos droits ! »

30 • La CNPD et l'APDL organisent une conférence sur les droits des citoyens et les nouveautés apportées par le règlement européen

FÉVRIER

7-8 • La CNPD organise des formations d'introduction à la protection des données

9 • La CNPD valide la charte « BCR » de PayPal

AVRIL

13 • La CNPD organise des workshops sur l'usage du GDPR Compliance Support Tool

MAI

3-4 • La CNPD participe à la conférence de printemps des autorités de protection des données à Tirana

25 • Entrée en application du règlement général sur la protection des données

25 • Le groupe de travail « Article 29 » au niveau européen est remplacé par le Comité Européen de la Protection des Données

29 • La CNPD lance la consultation publique concernant le schéma de certification « GDPR Carpa »

JUIN

4 • La CNPD organise la conférence « Four Decades of Data Protection » en présence du premier Ministre Xavier Bettel et de la Commissaire européenne Vera Jourova

6-10 • La CNPD distribue 12.000 exemplaires de sa brochure « Vos données ? vos droits ! »

8 • La CNPD organise un Cybersecurity Breakfast avec SECURITYMADEIN.LU sur les notifications des violations de données et les incidents de sécurité

29 • La CNPD publie une guidance générale en matière de protection des données pour les associations sans but lucratif

JUILLET

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

18 • La CNPD publie des lignes directrices sur l'exercice du droit à l'image

AOÛT

14 • La CNPD publie des lignes directrices en matière de vidéosurveillance

SEPTEMBRE

4 • La CNPD organise des sessions de formation d'introduction à la protection des données

OCTOBRE

10 • Le Luxembourg signe le protocole d'amendement à la Convention 108 du Conseil de l'Europe

22-26 • La CNPD participe à la 40e Conférence internationale des commissaires de la protection des données et de la vie privée à Bruxelles

NOVEMBRE

27 • La CNPD publie des lignes directrices relatives aux règles de protection des données dans le cadre des élections sociales

27-29 • La CNPD participe au séminaire européen « Case Handling Workshop » à Budapest

28 • La CNPD organise son premier DaProLab sur l'évaluation des impacts sur les personnes concernées d'une violation de données

DÉCEMBRE

10 • Journée internationale des Droits de l'Homme

L'ANNÉE 2018 EN UN COUP D'ŒIL

2

SENSIBILISATION, GUIDANCE ET CONSEIL

12.000
BROCHURES DISTRIBUÉES

lors de la campagne de sensibilisation « Vos données, vos droits »

12
FORMATIONS

d'introduction à la protection des données

86
PRÉSENTATIONS

lors de conférences, séminaires et tables rondes

2
WORKSHOPS

sur l'usage du GDPR Compliance Support Tool, un outil qui permet aux utilisateurs de vérifier le niveau de maturité de leurs organisations en matière de protection des données

1ER
DAPROLAB

Nouveau type d'événement permettant l'échange de vue sur un sujet spécifique entre professionnels de la protection des données

4
NOUVELLES GUIDANCES

- Vidéosurveillance
- Droit à l'image
- Guide pratique pour le monde associatif
- Élections sociales

27
AVIS

relatifs à des projets ou propositions de loi ou mesures réglementaires

+5 par rapport à 2017

1.112
DEMANDES DE RENSEIGNEMENT PAR ÉCRIT

Top 3 des questions concernent :
1. la vidéosurveillance
2. le délégué à la protection des données
3. le droit d'accès

+110% par rapport à 2017

CONFORMITÉ ET CONTRÔLE

450

RÉCLAMATIONS

Raisons principales :
1. Non-respect du droit d'accès (24%)
2. Demande d'effacement ou de rectification non respectée (16%)
3. Doutes quant à la licéité de certaines pratiques administratives ou commerciales (15%)

+125% par rapport à 2017

172

NOTIFICATIONS DE VIOLATIONS DE DONNÉES

Cause principale : erreur humaine (57%)

Nature des incidents :
1. données personnelles envoyées au mauvais destinataire (49%)
2. piratage, hacking (34%)
3. divulgation des données personnelles à la mauvaise personne (21%)

Plus de la moitié des incidents sont détectés dans les 48 heures après qu'ils soient survenus.

25

AUDITS

pour vérifier la conformité des organismes en matière de désignation et d'implémentation du rôle du délégué à la protection des données

12

ENQUÊTES SUR PLACE

dans les domaines de la vidéosurveillance, de la géolocalisation, de la publicité et du marketing

493

DÉLÉGUÉS À LA PROTECTION DES DONNÉES (DPO)

493 personnes physiques ou morales ont été déclarés auprès de la CNPD

+343 par rapport à 2017 où 150 personnes étaient agréées pour exercer l'activité de chargé de la protection des données (sous l'ancien régime de la loi de 2002).

818

RESPONSABLES DU TRAITEMENT ONT COMMUNIQUÉ LES COORDONNÉES DE LEUR DPO À LA CNPD

LES ACTIVITÉS EN 2018

3

1 SENSIBILISATION, GUIDANCE ET CONSEIL

1.1 ACTIONS DE SENSIBILISATION

A) 28 JANVIER 2018 : JOURNÉE DE LA PROTECTION DES DONNÉES

12ème 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 ». Le but est de sensibiliser les citoyens sur 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'ouverture 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.

CONFÉRENCE SUR LES DROITS DES CITOYENS ET LES NOUVEAUTÉS APPORTÉES PAR LE RÈGLEMENT EUROPÉEN

Dans le cadre de la 12ème Journée de la protection des données, la CNPD et l'APDL (Association pour la protection des données au Luxembourg) ont organisé une conférence sur les droits des citoyens et les nouveautés apportées par le règlement européen. La conférence a été suivie par la table ronde « La protection des données personnelles à la portée de tous ? ».

C'était l'occasion pour l'APDL de présenter la version luxembourgeoise de son spot vidéo de sensibilisation. La CNPD a présenté sa nouvelle brochure de sensibilisation du grand public.

BROCHURE « VOS DONNÉES ? VOS DROITS ! »

Le but de cette publication est de présenter les droits des citoyens en matière de protection des données et d'expliquer comment les faire valoir.

La brochure existe en version française et allemande. Elle est disponible sous forme imprimée et peut être téléchargée sur le site Internet de la CNPD.

Conférence sur les droits des citoyens et les nouveautés apportées par le règlement européen.

B) CAMPAGNE DE SENSIBILISATION « VOS DONNÉES ? VOS DROITS ! »

A l'occasion de l'entrée en application du nouveau règlement général sur la protection des données le 25 mai 2018, la CNPD a lancé sa campagne de sensibilisation « Vos données ? Vos droits ! ».

Du 25 mai au 11 juin, l'autorité de protection des données a organisé plusieurs événements, distribué 12.000 brochures et gadgets dans de nombreux endroits stratégiques du Grand-Duché et est intervenue dans l'émission « Wousst der schon? » de RTL.

4 JUIN 2018 : CONFÉRENCE « FOUR DECADES OF DATA PROTECTION »

Le 4 juin 2018, la CNPD a réuni de prestigieux orateurs afin de célébrer 4 décennies de protection des données à la Rockhal. L'entrée en application du paquet protection des données composé de la directive police justice et du règlement général sur la protection des données (ci-après RGPD) les 8 et 25 mai dernier, était au centre de tous les débats.

En introduction, Monsieur le premier Ministre Xavier Bettel s'est interrogé sur le symbole qu'incarnait l'entrée en application du RGPD. Après avoir évoqué comment il avait vécu la journée du 25 mai, il affirmait que l'innovation dans les nouvelles technologies et la protection des données n'étaient pas antinomique. Il a ensuite souligné que les Européens étaient les protagonistes de la protection des données à l'ère de la digitalisation.

La Commissaire européenne à la justice, aux consommateurs et à l'égalité des genres, Madame Vera Jourova quant à elle, a rappelé le rôle de l'Union européenne dans la protection des données. Elle a soutenu que le règlement général sur la protection des données n'est pas une révolution mais une évolution de bon sens.

Cinq étudiants au sein du Master en droit de l'espace, des communications et des médias de l'Université du Luxembourg ont partagé leur retour d'expérience sur l'application de la protection des données au quotidien tant sur le plan personnel que sur le plan professionnel. Ils ont fait part de leurs techniques pour protéger au mieux leurs données en partageant le moins possible leurs données à caractère personnel sur internet et en lisant les politiques de confidentialité. Ils sont également revenus sur les défis que posaient le RGPD aux PME.

LES ACTIVITÉS EN 2018

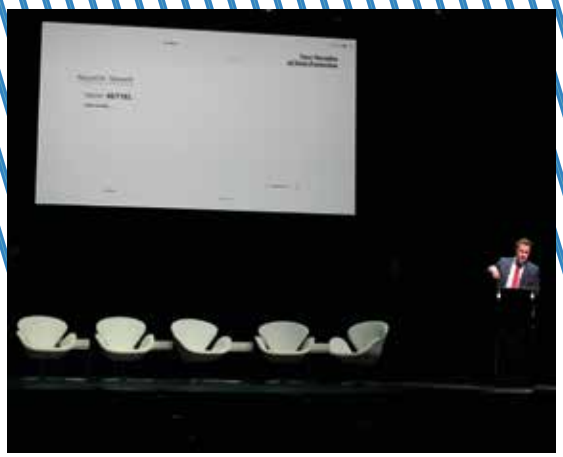
3

Tine A. Larsen, Xavier Bettel, Vera Jourova et Félix Braz lors de la conférence « Four Decades of Data Protection »

Le panel composé de Madame Andrea Jelinek, Présidente du Comité Européen de la Protection des Données (CEPD ou EDPB – European Data Protection Board), Monsieur Gérard Lommel, Commissaire du gouvernement pour la protection des données dans l'administration publique, et Prof. Mark D. Cole de l'Université du Luxembourg a effectué une rétrospective sur le rôle des autorités de la protection des données.

Le panel est revenu sur les premières années des autorités à la protection des données des États membres de l'Union européenne et les prémices de leurs coopérations au sein du groupe « Article 29 ». Ce dernier est remplacé par l'EDPB, qui continue son travail de coopération avec la lourde tâche de faire assoir l'application du paquet protection des données dans l'intérêt, tant des citoyens que des entreprises.

Monsieur Jan Philipp Albrecht, fervent défenseur de la vie privée et membre du Parlement européen, a adressé un message vidéo pendant la conférence. Il a fait état des étapes de négociation du paquet protection des données et sur le rôle important qu'a joué le Luxembourg lors de sa présidence au Conseil de l'Union européenne.



Conférence « Four Decades of Data Protection »

Monsieur Luc Reding, Conseiller de direction première classe au Ministère de la Justice, pour sa part s'est plus particulièrement arrêté sur l'implantation du paquet protection des données sous la présidence luxembourgeoise au Conseil de l'Union européenne. Son propos se penchait principalement sur la directive police-justice et le contexte de son adoption. Il a rappelé l'importance de la coopération en matière pénale et en matière d'investigations, mais qu'une telle coopération ne devait pas s'effectuer au détriment de la protection des données des victimes, des suspects et de l'ensemble des individus.

Me Jean-Louis Schiltz, Prof. Hon. à l'Université du Luxembourg et conseiller en droit des technologies, est notamment revenu sur les difficultés que rencontrent les PME dans la mise en œuvre du RGPD.

Madame Tine A. Larsen, présidente de la CNPD, a clôturé l'événement rappelant les missions de la Commission nationale pour la protection des données, à savoir sensibiliser et informer les citoyens sur la protection des données à caractère personnel mais aussi épauler et guider les entreprises dans la mise en œuvre du RGPD.

6-10 JUIN 2018 : DISTRIBUTION DE LA BROCHURE « VOS DONNÉES ? VOS DROITS ! »

Du 6 au 10 juin, la CNPD a distribué 12.000 exemplaires de sa brochure « Vos Données ? Vos Droits ! » et son gadget dans de nombreux endroits stratégiques du Grand-Duché.

8 JUIN 2018 : CYBERSECURITY BREAKFAST - NOTIFICATION 101 : HOW TO FACE DATA BREACHES AND SECURITY INCIDENTS ?

Le 8 juin, la CNPD a organisé un Cybersecurity Breakfast avec SECURITYMADEIN.LU sur les notifications des violations de données et les incidents de sécurité.

Depuis le 25 mai 2018, les responsables de traitement doivent notifier les violations de données à caractère personnel à la CNPD dans un délai de 72 heures après en avoir pris connaissance si la violation en question est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

Après un discours introductif de la présidente de la CNPD, une table ronde a rassemblé des experts en matière de la protection des données :

- Alain Herrmann - Head of Data Breach Unit and Certification Unit (CNPD)
- Gerard Wagener - CIRCL (Computer Incident Response Center Luxembourg)
- Dolores Peres - Head of Group Data Protection (KBL)
- Eric Romang - Data Protection and Information Security Officer (PingPong SA)

Distribution de la brochure « Vos Données ? Vos Droits ! »

4-9 JUIN 2018 : ÄER DONNEEËN ? ÄER RECHTER ! THÈME DE L'ÉMISSION « WOUSST DER SCHONN? » DE RTL

Du 4 au 9 juin, la CNPD est intervenue dans l'émission « Wousst der schonn? » de RTL Radio. Les droits existants, ainsi que les nouveaux droits en matière de protection des données y ont été présentés au grand public.

1.2 ORGANISATION DE FORMATIONS ET CONFÉRENCES

A) FORMATION « INTRODUCTION À LA PROTECTION DES DONNÉES »

En 2018, la CNPD a organisé 12 formations d'introduction à la protection des données en langue française et anglaise.

Plus de 500 personnes ont participé à ce séminaire destiné à les familiariser avec les notions de base essentielles, les droits 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.

B) FORMATION « LE PROFESSIONNEL EN PROTECTION DES DONNÉES PERSONNELLES »

La CNPD et la CSL ont allié leurs compétences pour l'élaboration d'un nouveau cours du soir : Le « professionnel en protection des données personnelles ».

Le public cible pour cette formation sont les responsables de traitement de données ou toute personne chargée de la protection des données personnelles.

Ce profil vise à comprendre les enjeux de la protection des données et les sources de risque potentielles, à partager des méthodes et des outils ainsi qu'à connaître les acteurs en support comme la CNPD. Les modules proposés apportent aux apprenants des connaissances solides sur la législation en vigueur, sur les systèmes d'information, sur la conformité et sur la communication. La formation-action permet quant à elle, par des mises en situation, aux apprenants d'acquérir de bons réflexes et de se constituer une boîte à outils.

Les modules composant ce profil sont :

- Gouvernance et compréhension des systèmes d'information
- Le cadre légal de la protection des données à caractère personnel et ses enjeux
- Formation-Action : les bonnes pratiques de la protection des données personnelles
- Sensibiliser et communiquer
- Audit et Compliance

Chaque module compte 25 heures réparties sur 10 séances à raison d'une soirée par semaine en dehors des congés scolaires luxembourgeois.

C) DAPROLAB (CNPD'S OPEN DATA PROTECTION LABORATORY)

En 2018, la CNPD a commencé à organiser de nouveaux événements intitulés « DaProLab (CNPD's Open Data Protection Laboratory) ».

Qu'est-ce que le DaProLab ?

- Une séance d'échanges d'idées, d'interprétations, de points de vue sur un sujet spécifique entre professionnels de la protection des données.
- Lors d'une séance de DaProLab, un seul sujet (défini à l'avance) est discuté.
- Dans le cadre de leur responsabilisation (« accountability »), les participants peuvent confronter leurs décisions /

prises de positions / points de vue / idées avec les autres participants afin d'obtenir un feedback quant à leurs choix effectués.
- Des échanges de connaissances et d'expériences.

Le premier DaProLab a eu lieu le 28 novembre 2018 et a porté sur l'évaluation des impacts sur les personnes concernées d'une violation de données dans le milieu hospitalier, des cabinets médicaux et laboratoires médicaux. Le représentant d'un hôpital national a présenté son approche. Cette dernière a servi de base pour lancer la discussion sur le sujet.

D) WORKSHOPS SUR L'USAGE DU GDPR COMPLIANCE SUPPORT TOOL

Afin d'aider les organisations dans leurs efforts de mise en conformité, la CNPD a développé un outil leur permettant de vérifier le niveau de maturité en matière de protection des données : le « GDPR Compliance Support Tool », disponible à l'adresse https://cst.cnpd.lu.

En 2018, la CNPD a organisé plusieurs workshops s'adressant principalement aux utilisateurs de cet outil. Les objectifs de ces événements étaient :

- d'expliquer le modèle de support à la conformité RGPD intégré à l'outil (organisation / traitements / sous-traitance) et comment ce modèle supporte l'exercice de la mise en conformité du responsable de traitement ;
- l'interactivité avec les participants pour répondre aux questions qui se posent quant à l'usage pratique de l'outil et à la compréhension des exigences à évaluer.

E) AUTRES ÉVÉNEMENTS AUXQUELS LA CNPD A PARTICIPÉ

À côté des événements mentionnées ci-dessus, 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.

Introduction à la protection des données
Tout au long de l'année, la CNPD a donné des cours d'introduction à la protection des données et ce notamment aux organismes suivants : la FEDAS (Fédération des Acteurs du Secteur Social au Luxembourg), l'European Mentoring & Coaching Council, l'ASBL femmes en détresse, le COSL (Comité Olympique du Sport Luxembourg), le CIJ (Centre national d'Information pour Jeunes), l'ASBL Familljencenter, les centres de rencontre pour jeunes de la Ville de Luxembourg, la FNEL (Fédération Nationale des Eclaireurs et Eclaireuses du Luxembourg), la RBS-Seniorenakademie et le SNJ (Service National de Jeunesse).

L'autorité de contrôle est également intervenue régulièrement auprès de l'Ecole Supérieure de Travail (EST) et de l'INAP afin de leur donner des formations générales sur la protection des données.

Des présentations axées sur les missions et pouvoirs de la CNPD ont par ailleurs été données à la Cour Grand-Ducale et lors de l'ERA Summer Course on European Data Protection Law.

Le nouveau règlement général sur la protection des données
En 2018, la CNPD a participé à de nombreux événements en lien avec les nouvelles règles en matière de protection des données afin de sensibiliser le maximum de personnes.

Des présentations plus générales concernant la conformité au RGPD ont notamment été données aux représentants du secteur communal, à la plateforme Jonk Handwierk, auprès du Groupement des Syndics Professionnels du Luxembourg, à l'Association luxembourgeoise des compliance officers (ALCO), à l'Ordre des Experts-Comptables, au collège vétérinaire et à Luxinnovation.

Lors d'autres conférences et formations, les sujets des présentations étaient plus spécifiques afin de tenir compte des besoins du public cible. Ainsi, la CNPD est intervenue :

- au troisième volet du cycle de conférences Fit4DataProtection organisé par la Chambre de Commerce et l'Enterprise Europe Network-Luxembourg sur les grands principes du RGPD et à un atelier en marge de la conférence intitulé « Testez votre conformité à l'aide du GDPR Compliance Support Tool » ;
- à la conférence « L'entreprise artisanale et les données personnelles » de la Chambre des Métiers sur les adaptations qu'une entreprise artisanale doit faire pour se conformer aux nouvelles règles ;
- à la « Computers, Privacy and Data Protection Conference » à Bruxelles lors du panel « Disruptive/Enabling technologies, ethics and the GDPR » ;
- au Data Privacy Day, organisé par RESTENA et l'Université du Luxembourg avec une présentation intitulée « Compliance monitoring by the CNPD » ;
- auprès de l'Ordre des architectes et des ingénieurs-conseils sur le thème « Protection des données et bureaux membres de l'OAI - l'équation à résoudre ensemble » ;
- lors d'une table ronde de l'Université du Luxembourg avec le titre « Help me, I'm hacked - Incident management and GDPR governance » ;
- lors d'un déjeuner avec l'AMCHAM (American Chamber of Commerce) et la BCC (British Chamber of Commerce) sur le thème des transferts des données vers les pays tiers et les nouveautés introduites par le RGPD ;
- à la conférence « Quel est l'impact concret du RGPD dans le domaine des ressources humaines ? » organisé par POG (Communauté RH au Luxembourg) ;

- lors de la conférence « Les services financiers dans un monde digital » de l'ALJB (Association luxembourgeoise des juristes en droit bancaire) avec un exposé sur le RGPD et les services financiers en ligne ;
- à l'événement « Delano Live : insights into the impact of the GDPR » en répondant aux questions du public ;
- lors d'un événement organisé par l'ABBL intitulé « Surfing the wave of the GDPR » avec une présentation sur « PSD 2 and the GDPR » ;
- auprès du CERT (Cyber Emergency Response Community) sur le sujet « Data Science/Engineering vs GDPR » ;
- lors de la conférence « Le RGPD : une stratégie de gouvernance au-delà de la protection ? » de par la Maison de l'Union européenne sur le thème « Les défis de l'application du RGPD au Luxembourg » ;
- au Luxembourg Data Protection Days « GDPR is now » avec une présentation intitulée « The enforcement approach of the CNPD » ainsi qu'une présentation au sujet de la certification et des codes de conduite;
- à un atelier pratique de l'House of Entrepreneurship sur le RGPD intitulé « Le RGPD, qu'est-ce que c'est ? Comment le mettre en place dans ma TPE ? » ;
- lors du Data Information Security Forum afin d'exposer les 7 étapes pour se mettre en conformité au RGPD ;
- lors d'un séminaire du Guichet Unique PME avec une présentation sur la façon dont les petites et moyennes entreprises peuvent se conformer à cette nouvelle législation ;
- à une conférence organisée en collaboration avec l'Association pour la Protection des Données au Luxembourg (APDL) et le Ministère de l'Economie sur la certification dans le cadre du Règlement général sur la protection des données ;
- à la conférence « Accountability in a GDPR World » de Grant Thornton Luxembourg avec un exposé sur le schéma de certification GDPR Carpa ;
- auprès de l'Entente des Offices Sociaux sur le rôle du délégué à la protection des données.

Autres thématiques

La CNPD a par ailleurs participé à des nombreuses conférences sur des thèmes plus spécifiques comme :

- la « RegTech » (Regulatory Technology) lors du CEPSlab18 sur le sujet « Technology : The missing link in compliance ? » et lors du RegTech Summit sur le thème « The state of the RegTech market : an outlook for compliance and regulations » ;
- l'intelligence artificielle dans la cadre d'une conférence du SnT (Interdisciplinary Centre for Security, Reliability and Trust) ;
- l'Internet des objets lors de l'Internet Security Day ;
- la santé dans le cadre d'une table ronde lors de la dixième conférence nationale de la santé intitulée « Innovation et santé digitale au service des citoyens : enjeux et défis » ;
- « L'exigence en matière de protection des données d'un consentement libre, spécifique, éclairé et univoque » lors de la journée d'éthique du Comité éthique hospitalier ;
- les violations de données lors du Cybersecurity Breakfast « Notification 101 : How to face data breaches and security incidents ? » ;
- les concepts de « Data protection by design » et « Data protection by default » auprès de Galexy.

LES ACTIVITÉS EN 2018

3

1.3 ÉLABORATION DE GUIDANCES

Toutes les guidances et lignes directrices peuvent être téléchargées sur le site Internet de la CNPD : www.cnpd.lu

Lignes directrices en matière de vidéosurveillance
Suite à l'entrée en application du RGPD, la CNPD a souhaité rappeler certains principes et certaines obligations applicables en la matière. Elle a par conséquent élaboré des lignes directrices qui s'adressent aux responsables du traitement souhaitant avoir ou ayant recours à des dispositifs de vidéosurveillance.

Contrairement à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données), le RGPD ne définit pas la notion de « surveillance ». De plus, une des conséquences directes du RGPD est qu'il n'est plus nécessaire de demander l'autorisation préalable de la CNPD pour installer un système de vidéosurveillance.

Dans ses lignes directrices, la CNPD a rappelé certains principes (principe de licéité du traitement, principe de finalité, principe de transparence, principe de nécessité et de proportionnalité) et certaines obligations applicables en matière de vidéosurveillance. L'autorité de contrôle y répond également à la question s'il faut effectuer une analyse d'impact relative à la protection des données en matière de vidéosurveillance.

Lignes directrices concernant le droit à l'image
Avec l'introduction du RGPD, la CNPD est régulièrement sollicitée au sujet de la licéité de la prise de vue et la publication de photos de personnes par rapport aux règles découlant de cette nouvelle législation. L'image d'une personne relève de la vie privée de cette personne et constitue une donnée à caractère personnel. L'image d'une personne est dès lors protégée par deux dispositifs juridiques, le droit à l'image tel que développé en application du droit au respect de la vie privée et le droit à la protection des données à caractère personnel découlant essentiellement du RGPD.

La CNPD a adopté ces lignes directrices pour clarifier les conditions générales de l'exercice du droit à l'image et de la protection de l'image en tant que donnée à caractère personnel. Elle entend répondre à deux questions principales :

- À quoi faut-il veiller quand on prend des photos ?
- Quelles précautions faut-il prendre en publiant des photos ?

Guide pratique pour le monde associatif
Ce guide vise à donner un aperçu et une guidance générale en matière de protection des données aux associations sans but lucratif.

Il s'adresse principalement et surtout aux associations dont l'activité se limite à effectuer des traitements de données habituels et nécessaires à la gestion d'une association dite « classique » ou « traditionnelle ».

Il n'est pas adapté à guider de manière exhaustive des associations qui de par la nature de leurs activités traitent des données personnelles (en termes de volume, de sensibilité, etc.) pour des finalités qui dépassent ce cadre habituel (p.ex. les associations sans but lucratif visées par la loi « ASFT » (loi modifiée du 8 septembre 1998 réglant les relations entre l'État et les organismes œuvrant dans les domaines social, familial et thérapeutique) qui œuvrent dans le domaine social, familial, thérapeutique, etc.).

Dans son guide, la CNPD aborde les points suivants :

- Rappel de quelques notions élémentaires
- L'établissement du registre
- La légitimité du traitement de données à caractère personnel
- L'information des personnes concernées

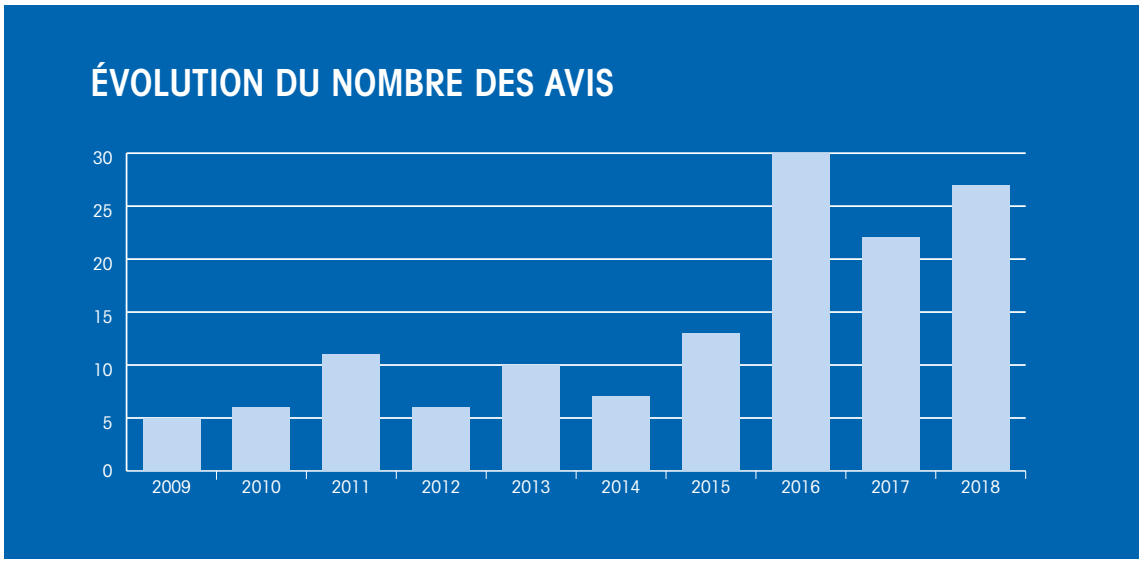
- Le respect des droits des personnes concernées
- Le délégué à la protection des données
- La sous-traitance
- Autres obligations plus spécifiques

Lignes directrices relatives aux règles de protection des données dans le cadre des élections sociales
Ces lignes directrices visent à guider les employeurs, partenaires sociaux et employés dans le contexte de l'organisation des élections sociales.

Suite aux changements législatifs en 2018, le système des autorisations préalables et des notifications préalables n'existe plus. Dans le contexte de l'organisation et du déroulement des élections des délégués du personnel et des représentants du personnel dans les conseils d'administration des sociétés anonymes, les employeurs ne peuvent donc plus soumettre un engagement formel de conformité relative à la décision de notification unique du 14 septembre 2007 (délibération n° 108/2007 - élections sociales), alors que celle-ci n'est plus prévue dans la législation en vigueur.

Nonobstant la suppression des formalités préalables à effectuer auprès de la CNPD, les principes et obligations définies par la législation applicable en matière de protection des données doivent néanmoins être respectés par les responsables du traitement.

Dans sa guidance, la CNPD explique les mesures à prendre par les employeurs ou les chefs d'établissement et décrit ce qu'il faut faire concernant les traitements de données en matière d'élections sociales.



1.4 AVIS ET RECOMMANDATIONS

Conformément à l'article 57, paragraphe 1er, lettre (e) du 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 »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la CNPD *« conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

LES ACTIVITÉS EN 2018

3

En 2018, la Commission nationale a émis 27 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

A) LUTTE CONTRE LE BLANCHIMENT ET CONTRE LE FINANCEMENT DU TERRORISME

Le 18 janvier 2018, la CNPD a avisé le projet de loi n° 7128 portant transposition des dispositions ayant trait aux obligations professionnelles et aux pouvoirs des autorités de contrôle en matière de lutte contre le blanchiment et contre le financement du terrorisme de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission.

Le projet de loi a pour objectif de modifier la législation luxembourgeoise actuelle, notamment la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme, afin de la rendre conforme aux nouvelles règles européennes, et plus particulièrement la Directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. Certains aspects de cette Directive et du projet de loi impliquent la collecte, l'analyse, la conservation et le partage de données à caractère personnel d'une multitude des personnes concernées tant par les professionnels tombant dans le champ d'application de la loi modifiée du 12 novembre 2004, que par les autorités chargées de la surveillance des professionnels.

En tenant compte de l'envergure du projet de loi, la Commission nationale a limité ses observations aux questions soulevées par les dispositions du projet de loi, causant des risques pour les personnes concernées ou apportant des changements suite à l'entrée en vigueur du RGPD ou de la Directive Police et Justice.

B) DONS D'ORGANES

Le 31 janvier 2018, la CNPD a émis un avis relatif au sujet de l'avant-projet de règlement grand-ducal relatif à l'organisation et les méthodes de travail du service national de coordination des dons d'organes.

Cet avant-projet de règlement grand-ducal a pour objet de définir l'organisation et les méthodes de travail du service national de coordination du prélèvement et de la transplantation d'organes. Ce service national de coordination a notamment pour mission de consigner sous forme électronique les données visées à l'annexe I du règlement grand-ducal du 27 août 2013 concernant la caractérisation, le transport et l'échange d'organes destinés à la transplantation. De plus, il établit et tient à jour une liste des coordinateurs impliqués dans la transplantation et le prélèvement d'organes, et une liste des malades en attente d'une greffe d'organes.

Dans son avis, la Commission nationale a abordé les points suivants : le rôle du responsable du traitement, les finalités du traitement, les catégories de données traitées, l'origine des données, les personnes ayant accès aux données et la durée de conservation des données.

C) EXÉCUTION EN MATIÈRE FISCALE DES DISPOSITIONS DU RGPD

Le 29 mars 2018, la Commission nationale s'est prononcée au sujet du projet de loi n°7250 portant exécution, en matière fiscale, des dispositions 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 et portant modification: 1) de la loi générale des impôts modifiée du 22 mai 1931 («Abgabenordnung») ; 2) de la loi modifiée du 29 mars 2013 relative à la coopération administrative dans le domaine fiscal ; 3) de la loi du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) ; 4) de la loi du 24 juillet 2015 relative à FATCA.

Selon l'exposé des motifs, ce projet de loi entend permettre à l'Administration des contributions directes (ci-après : « l'ACD ») de se prévaloir de certaines des limitations énoncées à l'article 23, paragraphe 2 du RGPD dans l'accomplissement des missions dévolues légalement à l'ACD, y compris les obligations découlant d'accords internationaux.

Au vu de la nature des dispositions contenues dans ce projet de loi, qui ont directement trait à la matière de la protection des données à caractère personnel, et plus particulièrement aux droits des personnes concernées, la Commission nationale a regretté dans son avis de ne pas avoir été formellement saisie du projet de loi par Monsieur le Ministre des Finances. Pour cette raison 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.

Dans une première partie générale, la CNPD a précisé l'étendue des limitations de l'article 23 du RGPD, et les garanties appropriées qui doivent être mises en place afin que les conditions des paragraphes 1er et 2 de cet article soient respectées.

Dans une seconde partie, elle a examiné plus en détail chacun des articles 1 et 2 du projet de loi, afin de déterminer si ceux-ci présentent des garanties appropriées. Enfin, elle a fait part de certains commentaires plus spécifiques, ayant trait aux articles 4 et 5 du projet de loi.

D) MISE EN PLACE DU DOSSIER DE SOINS PARTAGÉ

Le 5 avril 2018, la CNPD a émis un avis sur le projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé.

LES ACTIVITÉS EN 2018

3

Ce projet pose le cadre règlementaire applicable au dossier de soins partagé (ci-après « le DSP »). Il est pris en application de l'article 60quater du Code de la sécurité sociale, introduit par la loi du 17 décembre 2010 portant réforme du système de soins de santé.

Le projet de règlement grand-ducal détaille les modalités et conditions de mise en place du DSP. Il fixe ainsi les grands principes applicables à la création du DSP (article 2), à son activation et son accès par le titulaire dudit dossier (article 3), à sa fermeture et suppression (article 4), à l'accès au DSP par les professionnels de santé (article 5), aux droits d'accès, d'écriture et d'opposition du titulaire (article 6), aux titulaires mineurs non émancipés et titulaires majeurs protégés par la loi (article 7), aux droits d'accès et d'écriture des professionnels de santé (article 8), à la traçabilité des accès et des actions (article 9), au délai de versement des données au DSP (article 10), à la sécurité de la plateforme électronique nationale (article 11), aux modalités techniques de versements des données au DSP et interopérabilité (article 12) et à la coopération et échanges transfrontaliers (article 13).

La Commission nationale a limité ses observations aux dispositions du projet de règlement grand-ducal ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel. La CNPD s'est

prononcée notamment sur la base de légitimité de la création du DSP, la question de la responsabilité du traitement, la question des sanctions, la création, l'activation, la fermeture et la suppression du DSP, l'accès par le titulaire et par les professionnels de santé, la traçabilité des accès et des actions, le délai de versement des données au DSP et la sécurité de la plateforme électronique nationale.

E) RÉORGANISATION DU SERVICE DE RENSEIGNEMENT DE L'ÉTAT

En 2018, la CNPD a publié deux avis complémentaires relatif au projet de règlement grand-ducal pris en exécution de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

En 2016, la CNPD avait déjà rendu son avis relatif au projet de règlement grand-ducal pris en exécution de la future loi portant réorganisation du Service de Renseignement de l'État et au projet de règlement grand-ducal pris en exécution de la loi du 15 juin 2004 relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité.

Par courrier du 18 décembre 2017, Monsieur le Premier Ministre avait invité la Commission nationale à se prononcer au sujet des amendements apportés au projet de règlement grand-ducal susmentionné.

Dans son avis, la Commission nationale avait rappelé qu'un premier avant-projet de règlement grand-ducal portant création et fixant les modalités de fonctionnement d'un fichier relatif au traitement de données à caractère personnel par le Service de Renseignement de l'État avait déjà été soumis à la CNPD pour avis en 2013 et a donné lieu à l'avis de la Commission nationale pour la protection des données relatif à l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'État et à l'avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

Dans ses avis complémentaires de 2018, la Commission nationale a passé en revue les amendements qui ont donné lieu à observations concernant notamment les catégories de données à caractère personnel traitées par le Service de renseignement de l'État, la durée de conservation des données, l'accès aux données par les agents du SRE et la journalisation des données.

F) ORGANISATION DE LA CNPD ET MISE EN ŒUVRE DU RGPD

En 2018, la CNPD a rendu deux avis complémentaires relatif aux amendements gouvernementaux 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'État 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 le premier avis du 25 avril 2018, la CNPD a limité ses observations à l'amendement n° 28 qui insère un nouvel article 71 dans le projet de loi. Ce nouvel article 71 a pour objet de remplacer l'article L. 261-1 du Code du travail par un nouveau texte. La Commission nationale s'est posée plusieurs questions fondamentales quant au maintien de cette disposition ainsi qu'à sa conformité à la jurisprudence européenne et au RGPD.

Le 8 juin 2018, la CNPD a adopté un deuxième avis suite à une série d'amendements parlementaires, adoptés en date du 14 mai 2018.

G) RENITA

Le 27 avril 2018, la CNPD a avisé le projet de loi n° 7248 relatif au financement des travaux d'extension et de perfectionnement du Réseau national intégré de radiocommunication pour les services de sécurité et de secours luxembourgeois et portant modification de la loi du 20 mai 2014 relative au financement du Réseau national intégré de radiocommunication pour les services de sécurité et de secours luxembourgeois.

Suivant l'exposé des motifs, le projet de loi vise d'une part, à renforcer les moyens financiers afin d'« accueillir de nouveaux utilisateurs et de perfectionner le fonctionnement du réseau » et d'autre part, « à conférer un fondement légal au traitement des données à caractère personnel concernant les agents publics des autorités, administrations et organismes publics découlant de l'utilisation des équipements et services de communication RENITA ».

Au regard du nombre élevé d'agents concernés et du risque d'atteinte au respect de la vie privée des agents sur leur lieu de travail, la Commission nationale a accueilli favorablement que le gouvernement entend fonder le traitement des données personnelles traitées via le réseau RENITA dans le droit national.

Dans le cadre de son avis, la Commission nationale s'est limitée à formuler quelques observations relatives à l'article 3 du projet de loi qui insère un nouvel article 5 à la loi du 20 mai 2014 précitée. Les observations concernent entre autres les responsables du traitement, les finalités du traitement, les modalités d'accès aux données à caractère personnel, la durée de conservation des données de géolocalisation GPD, de trafic CDR et d'enregistrement des messages et conversations.

H) VENTE PAR INTERNET AU PUBLIC DE MÉDICAMENTS À USAGE HUMAIN

Le 9 juillet 2018, la CNPD a avisé le projet de règlement grand-ducal concernant : 1. la vente par internet au public de médicaments à usage humain; 2. la préparation, la division, le conditionnement ou le reconditionnement des médicaments à usage humain.

Le projet de règlement grand-ducal vise à exécuter la loi du 7 juin 2017 modifiant la loi modifiée du 4 août 1975 concernant la fabrication et l'importation des médicaments et 2. la loi modifiée du 25 novembre 1975 concernant la délivrance au public de médicaments.

D'après l'exposé des motifs, ce projet comporte deux volets :

1. les modalités de la mise en œuvre des règles de qualité et de sécurité encadrant les opérations de préparation, de division, de conditionnement ou de reconditionnement des médicaments en officine ou en pharmacie hospitalière ;

2. les modalités de la mise en œuvre de la vente à distance au public de médicaments non soumis à prescription médicale en vue d'adapter la législation en matière de médicaments à usage humain au droit européen.

La Commission nationale a limité ses observations aux dispositions du projet de règlement grand-ducal ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel. Elle a abordé les problématiques de la sous-traitance, des responsabilités et des compétences du personnel et du compte électronique personnel.

I) CRÉATION DE L'AUTORITÉ NATIONALE DE SÉCURITÉ

Le 16 juillet 2018, la CNPD a avisé le projet de loi n° 6961 portant 1. création de l'Autorité nationale de sécurité (ci-après « ANS ») et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2) du Code pénal.

Auparavant, en 2013, la CNPD avait déjà rendu un avis relatif à un avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

Dans l'avis de 2018, la Commission nationale a commenté plusieurs amendements, notamment concernant les bases de données auxquelles l'ANS peut accéder, la durée de conservation ou encore les fichiers de journalisation.

J) MODERNISATION DU DROIT DE LA FAILLITE

Le 16 juillet 2018, la CNPD a donné son avis relatif au projet de loi n° 6539 relatif à la préservation des entreprises et portant modernisation du droit de la faillite.

Le 20 novembre 2015, la CNPD avait déjà rendu un premier avis relatif à ce projet de loi dans lequel elle a formulé différentes observations concernant notamment la problématique des données judiciaires, la collecte des données sur les entreprises en difficulté, le droit d'accès, la création d'une base légale pour la transmission de certains jugements au (secrétariat du) Comité de conjoncture, la demande de communication d'informations de la part du (secrétariat du) Comité de conjoncture et la problématique de la liste des protêts.

Dans l'avis de 2018, la Commission nationale a limité ses observations aux amendements qui ont donné lieu à des observations en rapport avec le respect de la vie privée et avec la protection des données à caractère personnel. Plus précisément, ces amendements concernaient la détermination du ou des responsables du traitement, les finalités des traitements de données à caractère personnel et la nature et les catégories de données traitées.

K) ACTIVITÉ D'ASSISTANCE À L'INCLUSION DANS L'EMPLOI

Le 16 juillet 2018, la CNPD a donné son avis concernant le projet de loi n° 7269 complétant le Code du travail en portant création d'une activité d'assistance à l'inclusion dans l'emploi pour les salariés handicapés et les salariés en reclassement externe.

D'après l'exposé des motifs, ce projet de loi vise « à faciliter l'intégration, et surtout le maintien dans l'emploi des personnes ayant le statut de salarié handicapé ou étant en reclassement externe, par la création d'une activité appelée « assistance à l'inclusion dans l'emploi ».

La Commission nationale a limité 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.

Elle a notamment salué le degré de détail avec lequel les auteurs du projet de loi ont précisé les données à caractère personnel que le formulaire de demande d'assistance à l'inclusion dans l'emploi établi par l'Agence pour le développement de l'emploi (ADEM) devait contenir.

En prenant en compte les principes de licéité et de sécurité juridique, la CNPD a suggéré aux auteurs du projet de loi de préciser dans le corps du texte la durée de conservation des données contenues dans le fichier d'assistance. En effet, l'article 5, paragraphe (1), lettre (e) du RGPD impose au responsable de traitement de veiller à ce que les données qu'il traite ne soient pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

L) CONTENU MINIMAL DU DOSSIER INDIVIDUEL DU PATIENT HOSPITALIER ET DU RÉSUMÉ CLINIQUE DE SORTIE

Le 19 octobre 2018, la CNPD a avisé le projet de règlement grand-ducal déterminant le contenu minimal du dossier individuel du patient hospitalier et du résumé clinique de sortie.

D'après l'exposé des motifs, ce projet de règlement grand-ducal vise à uniformiser le contenu du dossier individuel du patient hospitalier, ainsi que du résumé clinique de sortie. En effet, l'article 37 de la loi du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière prévoit la mise en place dudit dossier hospitalier qui est censé retracer, de façon chronologique et fidèle, l'état de santé du patient et son évolution au cours de la prise en charge. L'article en question précise que « le contenu minimal du dossier individuel du patient hospitalier et du résumé clinique de sortie est déterminé par règlement grand-ducal, l'avis de la Commission nationale pour la protection des données ayant été demandé. »

Dans son avis, la CNPD a notamment abordé les problématiques du contenu du dossier hospitalier, du champ d'application, de l'identification du patient et de l'accessibilité du dossier.

M) REGISTRE DES BÉNÉFICIAIRES EFFECTIFS

Le 22 novembre 2018, la CNPD a avisé le projet de loi n° 7217 instituant un Registre des bénéficiaires effectifs et portant transposition de plusieurs dispositions de directives européennes.

Selon l'exposé des motifs, le projet de loi entend adapter la législation luxembourgeoise aux exigences internationales en matière de transparence des personnes morales qui découlent de l'article 30 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission.

Le projet de loi vise à instituer un registre central concernant des bénéficiaires effectifs ayant pour mission la conservation et la mise à disposition des informations sur les bénéficiaires effectifs des personnes morales.

Ayant déjà été consultée par le ministère de la Justice au stade d'avant-projet de loi analysé, la Commission nationale s'est limitée à formuler les observations sur les rôles et responsabilités du responsable du traitement, les entités immatriculées, les données conservées par les entités immatriculées, les données figurant au registre, l'accès aux données contenues dans le registre, la durée de conservation et les droits des personnes concernées.

N) SANCTIONS ADMINISTRATIVES COMMUNALES

Le 7 décembre 2018, La CNPD a donné son avis concernant le projet de loi n° 7126 relatif aux sanctions administratives communales modifiant 1) le Code pénal, 2) le Code de procédure pénale, et 3) la loi communale modifiée du 13 décembre 1988.

L'objectif principal du projet de loi est de faire *« face au besoin des communes de disposer d'un instrument leur permettant de lutter contre la petite délinquance, les actes de vandalisme et autres incivilités que le droit pénal et les organes répressifs ne permettent plus d'endiguer efficacement (…) ».*

Pour sa part, la Commission nationale a limité 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. Ses observations concernaient notamment l'accès du fonctionnaire sanctionnateur au registre national des personnes physiques et la création des registres des sanctions administratives communales.

O) DÉCLARATION OBLIGATOIRE DE CERTAINES MALADIES

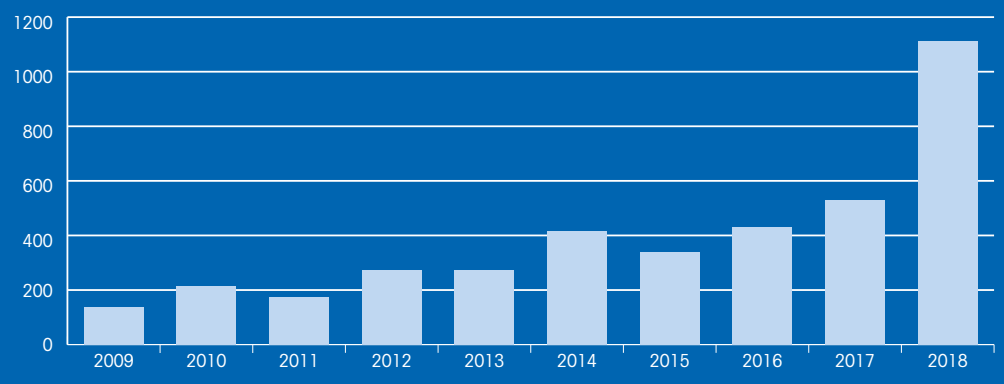
Le 7 décembre 2018, la Commission nationale a avisé le projet de règlement grand-ducal portant exécution de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

Le projet de règlement grand-ducal a comme objet de dresser une liste des maladies à déclaration obligatoire et des maladies présentant une menace grave pour la santé publique, ainsi que le délai endéans duquel la déclaration doit être faite au directeur de la Santé ou à son délégué par les médecins, les médecins-dentistes et les responsables des laboratoires d'analyses médicales.

Dans son avis, la CNPD s'est prononcée concernant :

- la base de légitimité de la création d'un système centralisé des maladies infectieuses ;
- les données à caractère personnel destinées à figurer dans le système centralisé ;
- le traitement de données génétiques ;
- les droits des personnes concernées et la durée de conservation des données et
- l'accessibilité au système centralisé et à la mise en place de mesures de sécurité appropriées.

ÉVOLUTION DU NOMBRE DE DEMANDES DE RENSEIGNEMENT PAR ÉCRIT



1.5 TRAITEMENT DES DEMANDES DE RENSEIGNEMENTS

La Commission nationale a reçu 1.112 demandes de renseignement par écrit en 2018, soit plus que le double qu'en 2017 où elle en avait reçu 528.
La raison principale de l'augmentation des sollicitations est l'entrée en application du nouveau règlement général sur la protection des données le 25 mai 2018. La CNPD a reçu de nombreuses questions sur la mise en conformité à la nouvelle législation tout au long de l'année et plus particulièrement pendant les mois de mai et de juin.

Environ deux tiers 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.

Les thématiques qui reviennent le plus souvent sont les suivantes :

- la vidéosurveillance (y compris vidéosurveillance du domicile privé et vidéosurveillance sur le lieu de travail) ;
- le délégué à la protection des données (son rôle, les conditions pour être nommé, la procédure pour déclarer un DPO auprès de la CNPD) ;
- le droit d'accès (pour les personnes concernées : comment exercer mon droit d'accès ? et pour les responsables de traitement : comment et dans quelles conditions faire droit à une demande d'accès ?) et les autres droits des personnes concernées (droit à l'effacement des données, droit d'opposition, droit de rectification, etc.).

D'autres questions récurrentes concernent notamment :

- le champ d'application territorial du RGPD (pour les sociétés établies en dehors de l'UE, y compris les questions liées à la désignation d'un établissement principal ou unique et d'une autorité de contrôle principale) ;

- les certifications (Quel est le champ d'application de la certification « GDPR-CARPA » ?) ;
- l'anonymisation et la pseudonymisation des données à caractère personnel (et leur impact concernant les règles applicables en matière de protection des données) ;
- le consentement des personnes concernées (Dans quels cas et sous quelles conditions doit-il être demandé ?) ;
- les cookies (Quelles sont les règles pour les hébergeurs de sites internet utilisant des cookies ?) ;
- les violations de données (Qu'est-ce qui constitue une violation de données et à partir de quel moment faut-il notifier la CNPD ?) ;
- le droit à l'image (pour les ASBL, sur les réseaux sociaux, en milieu scolaire, etc.) ;
- les drones (pour les personnes concernées : un drone a survolé ma propriété, quels sont mes moyens d'actions ? pour les responsables de traitement : dans quelles conditions et où puis-je piloter un drone et filmer à l'aide de celui-ci ?) ;
- les questions liées à l'utilisation du « GDPR Compliance Support Tool » de la CNPD ;
- la durée de conservation des données (Combien de temps a-t-on le droit de conserver les données à caractère personnel de nos clients ? ou de nos employés ?) ;
- la prospection / le marketing (Dans quelles conditions pouvons-nous envoyer des newsletters ou mails publicitaires à nos clients ?) ;
- les ressources humaines (Dans quelles conditions un potentiel employeur peut-il se renseigner auprès de l'ancien employeur d'un candidat ?) ;
- la sous-traitance (Quelles sont les conditions liées au recours à un sous-traitant ? Est-ce que la CNPD dispose de modèles de contrats de sous-traitance ?) ;
- l'utilisation du numéro de matricule (Dans quelles conditions pouvons-nous utiliser le numéro de matricule de nos employés ou de nos clients ?) ;
- les dashcams (L'utilisation de dashcams est-elle admise ou interdite au Luxembourg ?).

LE SYSTÈME D'INFORMATION DU MARCHÉ INTÉRIEUR (IMI)

Depuis le 25 mai 2018, le système IMI est la plate-forme informatique qui garantit la bonne mise en œuvre de la coopération entre les autorités de contrôle telle que stipulé dans le règlement général sur la protection des données (RGPD). Les autorités de contrôle des États membres doivent coopérer étroitement pour assurer une protection uniforme des droits des personnes en matière de protection des données dans l'ensemble de l'Union européenne.

Aujourd'hui, plus que jamais, l'assistance mutuelle et la coordination de la prise de décision dans les affaires transfrontières de protection des données sont de la plus haute importance.

En outre, le Comité européen de la protection des données émet des avis et prend des décisions contraignantes lorsque des autorités nationales de protection des données ont des positions différentes dans une affaire transfrontière.

Ce degré élevé de coopération administrative dans toute l'Europe se déroule maintenant par l'intermédiaire du système IMI.

A l'aide du système IMI, les autorités de contrôle pourront notamment :

- déterminer quelle est l'autorité de contrôle chef de file dans un litige transfrontalier ;
- coopérer pour parvenir à un règlement des litiges transfrontaliers ;
- demander et fournir une assistance aux autorités de contrôle d'autres États membres ;
- organiser des opérations communes associant les autorités de contrôle de plusieurs États membres.

2 CONFORMITÉ ET CONTRÔLE

2.1 TRAITEMENTS DES RÉCLAMATIONS

Si une demande d'un particulier auprès d'un responsable du traitement est restée sans suite, ceux-ci peuvent s'adresser à la CNPD. Le traitement des réclamations émanant des personnes concernées compte parmi ses missions.

En 2018, la CNPD a reçu 450 réclamations :

- 376 personnes ont directement 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.
- 74 plaintes ont été transmises à la CNPD par le système d'information du marché intérieur (IMI).

Le nombre de réclamations a ainsi plus que doublé par rapport à l'année précédente, de 200 en 2017 à 450 en 2018.

LES ACTIVITÉS EN 2018

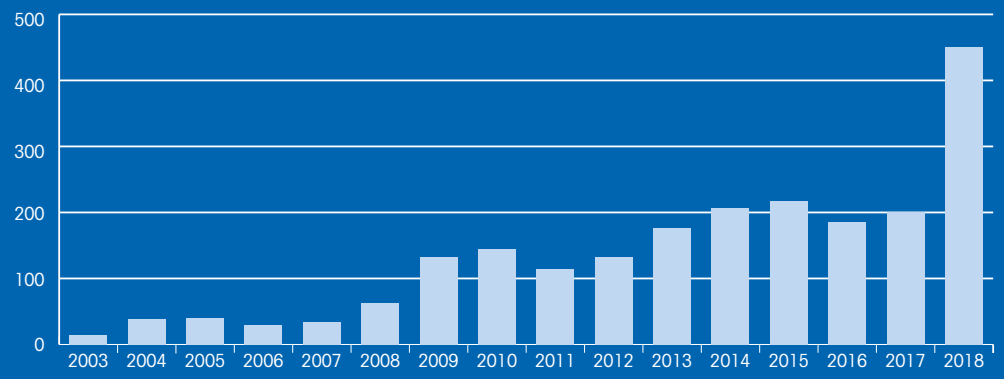
3

L'entrée en application du RGPD le 25 mai 2018 a eu un impact important sur le nombre de plaintes reçues par la CNPD. Lors des 5 premiers mois de l'année, la CNPD a reçu en moyenne 18 plaintes par mois, tandis que pour les 7 prochains mois, elle en a reçu 51 par mois.

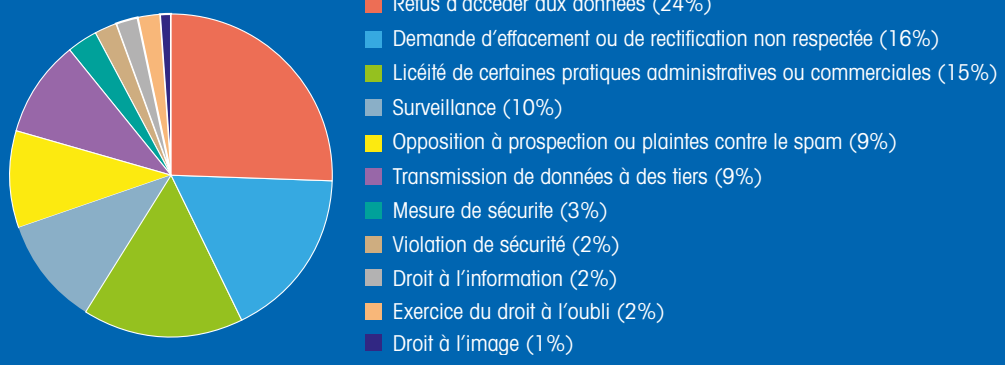
Presqu'un quart des plaintes (24%) a été motivé par le non-respect du droit d'accès par les responsables du traitement. Ceux-ci ont refusé aux citoyens d'accéder à leurs données, ignoré leurs requêtes ou ne leur ont pas donné assez de renseignements par rapport aux obligations légales à respecter en 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 16% des plaintes reçues en 2018. Il s'agissait, 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.) accessibles sur des sites Internet.

ÉVOLUTION DU NOMBRE DE RÉCLAMATIONS



MOTIFS DES RÉCLAMATIONS



Dans 15% des cas, les plaignants ont demandé à la CNPD de vérifier la licéité de certaines pratiques administratives ou commerciales. Ils ont notamment remis en cause :

- les conditions générales 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 (p.ex. sur un réseau social) ;

- la collecte illicite ou excessive de données ;
- la licéité de traitement des dossiers du personnel ;
- la création d'annuaires sans le consentement des personnes concernées ;
- la prise de photos à l'insu de la personne concernée ;
- les décisions individuelles automatisées.

La majorité des requêtes liées à la surveillance sur le lieu du travail (10% des plaintes) concernaient la vidéosurveillance. Des plaignants ont également contacté la CNPD lorsqu'ils ont estimé que des systèmes de géolocalisation avaient été utilisés par leur employeur de manière illicite (p.ex. surveillance en dehors des heures de travail).

9% 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.

La transmission non autorisée de données à des tiers a également conduit à un certain nombre de réclamations (9%). 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.

2.2 CONTRÔLES EFFECTUÉS

La CNPD a renforcé sa méthodologie d'enquête en 2018 afin de contrôler au mieux le respect du RGPD (élaboration d'une stratégie annuelle, réalisation d'analyses de risques thématiques générales et spécifiques, etc.).

Dans la mesure où le RGPD exige un haut degré de transparence des responsables de traitement et sous-traitants envers les personnes concernées et les autorités de contrôle, la CNPD a estimé qu'il est de son devoir d'appliquer de son côté une transparence accrue dans le cadre de l'exécution de ses missions.

Pour veiller au respect de la législation applicable en matière de protection des données, la Commission nationale dispose de pouvoirs d'enquête au titre desquels elle peut :

- obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel qui sont traitées et à toutes les informations nécessaires à l'exercice de ses missions ;

- 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 ;
- mener des enquêtes sous la forme d'audits sur la protection des données.

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

Il y a deux types d'intervention :
- les contrôles sur place
- les audits sur la protection des données

A) CONTRÔLE SUR PLACE

La CNPD réalise des contrôles sur place proactifs ou réactifs sur base d'incidents, de réclamations, d'informations relayées dans les médias ou faisant suite à un contrôle précédent. Ces contrôles sont conduits à une échelle « individuelle » en fonction des faits qui auront été rapportés à la CNPD. Ils ne s'adressent donc qu'aux responsables de traitement concernés par les faits rapportés.

12 enquêtes sur place ont eu lieu en 2018 dans les domaines de la vidéosurveillance, de la géolocalisation, de la publicité et du marketing.

B) AUDITS SUR LA PROTECTION DES DONNÉES

Dans le cadre de l'entrée en application depuis le 25 mai 2018 du RGPD, CNPD a adapté sa stratégie et mis en place des enquêtes dites « proactives ». Ces enquêtes sont effectuées sous la forme d'audits thématiques portant sur les obligations du RGPD. Ces audits sont menées dans plusieurs organismes et vont permettre à la CNPD d'évaluer le niveau de conformité des organismes au RGPD.

Pour réaliser ces audits, la CNPD se base notamment sur les documents d'orientations générales fournis par le Comité Européen de la Protection des Données (« European Data Protection Board » ou EDPB en anglais) tels que les lignes directrices, les recommandations et les bonnes pratiques à propos du RGPD.

Vu l'impact du nouveau rôle du délégué à la protection des données et l'importance de son intégration dans l'entreprise, et considérant que des lignes directrices de l'EDPB à ce sujet sont disponibles depuis décembre 2016, la CNPD a décidé de lancer un audit thématique sur la fonction de délégué à la protection des données (DPD). Ainsi, 25 procédures d'audit ont été ouvertes en 2018.

L'objectif de cette campagne est de vérifier la conformité des organismes aux obligations du RGPD en matière de désignation du DPD, de ses missions et de ses fonctions.

La sélection des entités dans lesquelles cet audit est mené a été basée sur les critères suivants :

- la taille de l'organisme,
- la sensibilité des données traitées et
- le secteur d'activité.

Il est prévu de publier les résultats des audits anonymisés sous forme de lignes directrices afin de servir de bons exemples ou d'exemples à éviter à d'autres responsables de traitements ou sous-traitants intéressés.

2.3 NOTIFICATION DES VIOLATIONS DE DONNÉES

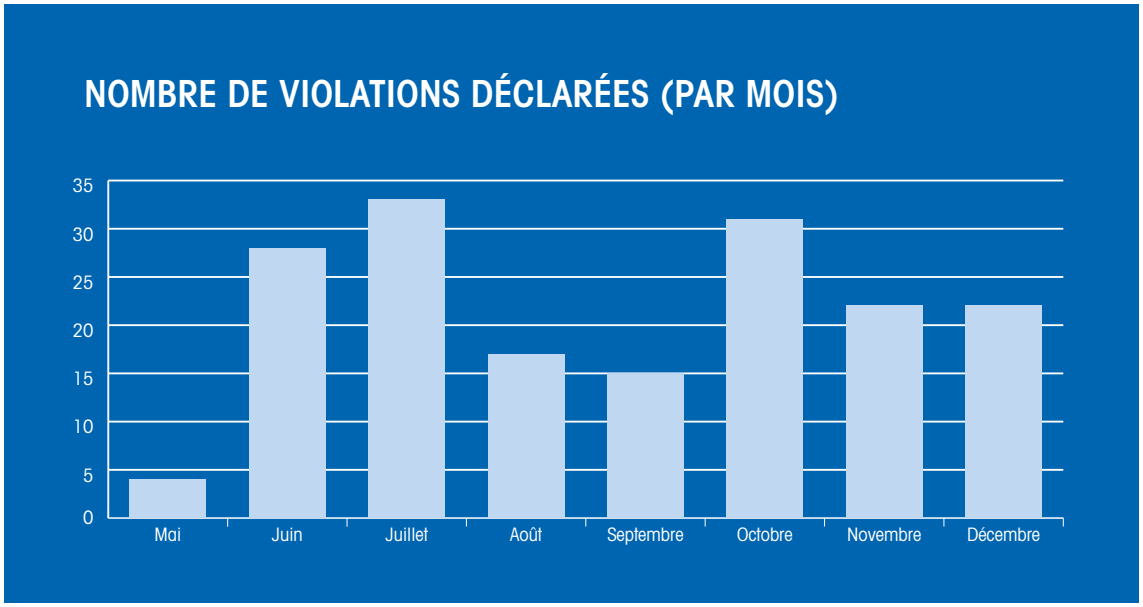
Deux types de violations de données doivent être notifiées à la CNPD :

- les violations de données dans le cadre du règlement général sur la protection des données et
- les violations de données dans le secteur des communications électroniques.

A) VIOLATIONS DE DONNÉES DANS LE CADRE DU RGPD

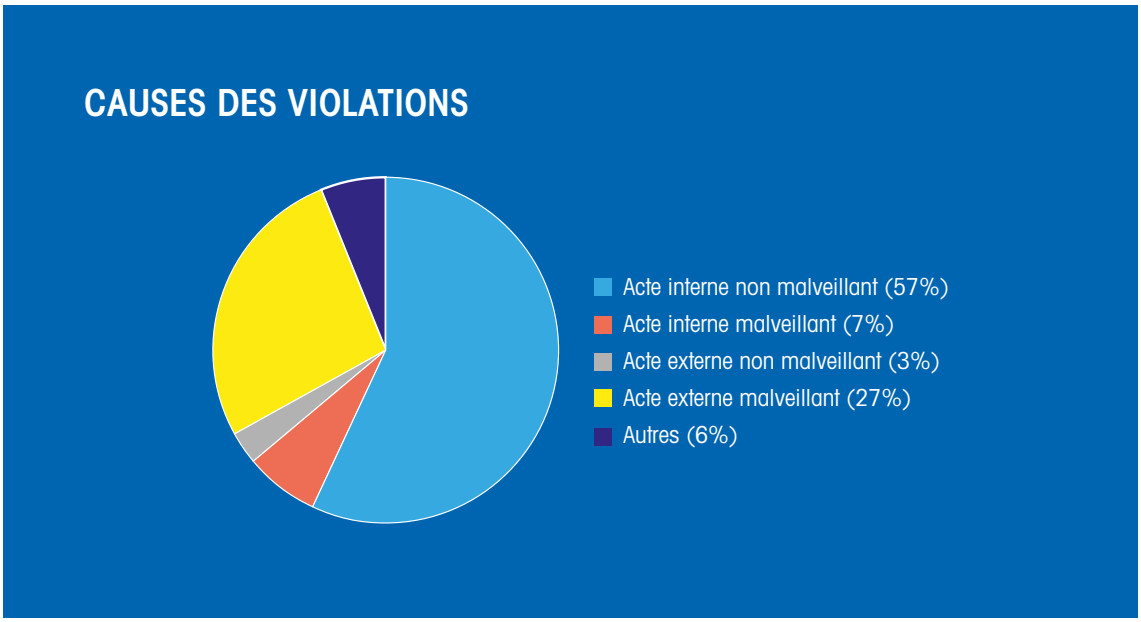
Depuis le 25 mai 2018, une violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel doit être gérée en respect des exigences des articles 33 et 34 du règlement général sur la protection des données (RGPD).

Les responsables de traitement doivent notifier les violations de données à caractère personnel à la CNPD dans un délai de 72 heures après en avoir pris connaissance si la violation en question est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.



Les statistiques suivantes sont basées sur les violations de données à caractère personnel qui ont été notifiées à la CNPD. Elles ne reflètent pas le nombre complet d'incidents de sécurité en rapport avec des données à caractère personnel. Les responsables de traitement sont tenus de maintenir une documentation de tous les incidents de sécurité impliquant des données à caractère personnel.

172 violations de données ont été notifiées à la CNPD entre le 25 mai et le 31 décembre 2018.



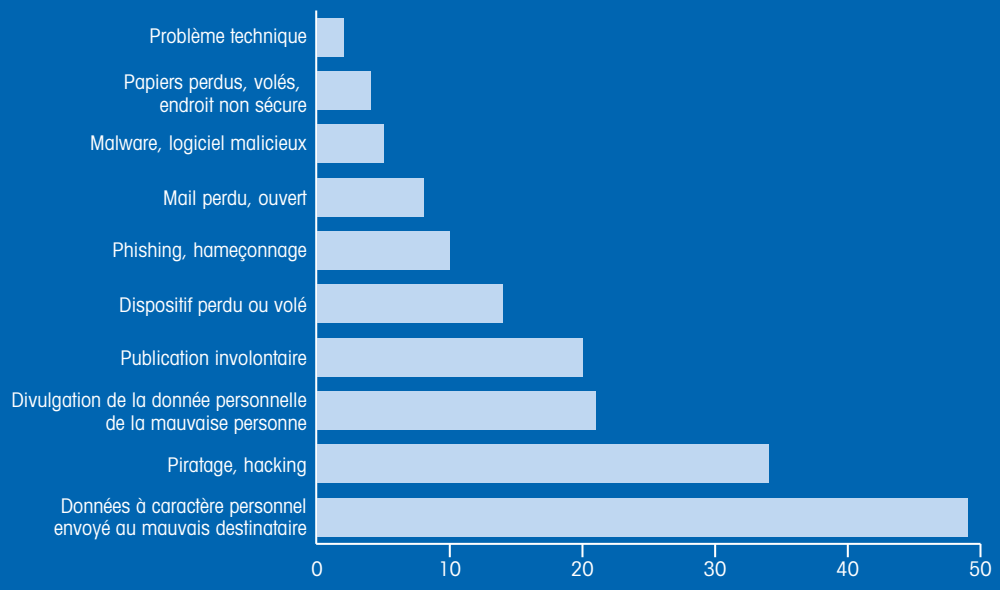
La principale cause de violation de données à caractère personnel reste l'erreur humaine (acte interne non malveillant).

La plupart des erreurs humaines se produisent :

- lorsqu'une procédure existante n'est pas suivie ;
- lorsqu'une règle de sécurité existante est contournée: ce type de cas a fait l'objet d'incidents aux conséquence importantes ;
- lorsque le personnel n'est pas assez sensibilisé aux règles de confidentialité à appliquer ;
- suite à une erreur d'inattention : dépendant du contexte, la mise en place d'un mécanisme de contrôle avant transmission des données (ex : principe des 4 yeux) aurait permis d'éviter ce type d'incident.

Des actes externes malveillants sont à l'origine de plus du quart des violations notifiées. Ce type d'incidents a

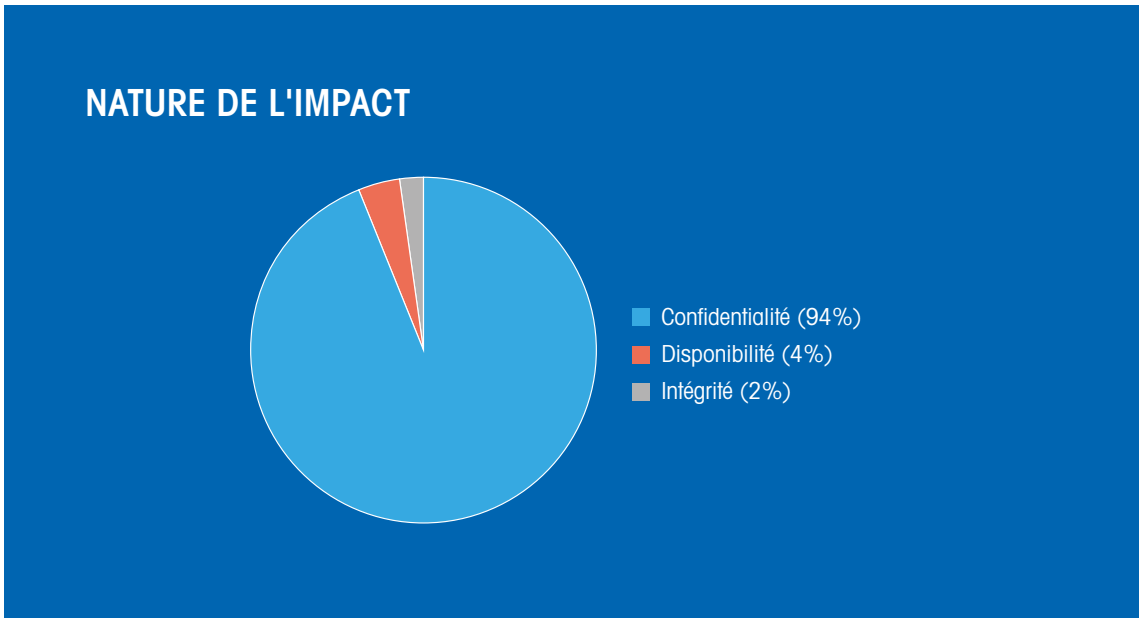
NATURE DES INCIDENTS



souvent un impact plus important sur les personnes concernées. Dans de nombreux cas, ces actes ciblent l'accès ou l'obtention de données qui permettent de réaliser des transactions financières à l'insu des personnes concernées (ex : interception de données de cartes de paiement bancaire, phishing pour obtenir les informations de connexions à un service de paiement, usurpation d'identité pour effectuer une transaction financière, etc.).

Les actes internes malveillants se sont produits principalement lors de départs, volontaires ou non, d'employés d'une organisation: cette situation amène des personnes à copier des données pour potentiellement les utiliser dans leur nouvelle situation. De même, les situations de cessation d'activité / fusion / rachat de sociétés sont des périodes à risque pour des exfiltrations non autorisées de données.

Les autres cas de figure sont liés à des bugs techniques qui résultent souvent dans la divulgation de données à caractère personnel à des tiers non autorisés (ex : mise en place ou mise à jour d'un nouveau service en ligne, cas non prévu d'utilisation d'un service, …).

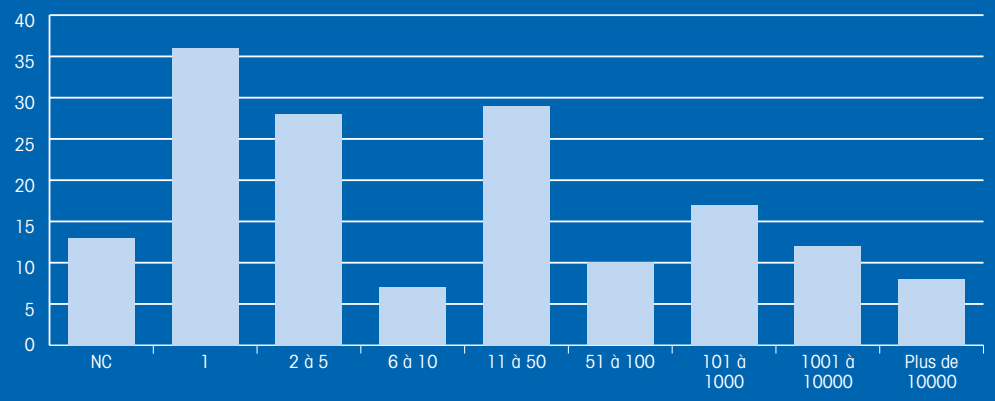


La quasi-totalité des violations de données ont un impact en rapport avec la perte de confidentialité des données concernées.

Plus de la moitié des incidents de sécurité sont détectés dans les 48 heures après de leur survenance. Toutefois, la CNPD a constaté que presque 18% des violations de données à caractère personnel ne sont détectées qu'au minimum un mois après s'être produites: il s'agit plus particulièrement d'incidents liés à des violations continues de la politique de sécurité de l'organisation (p.ex. : le personnel de direction envoie les données professionnelles sur leur email personnel pour travailler du domicile et l'email personnel est piraté), de données utilisées par des employés lors d'un départ d'une organisation et également de vol de données liée à des piratages non détectés.

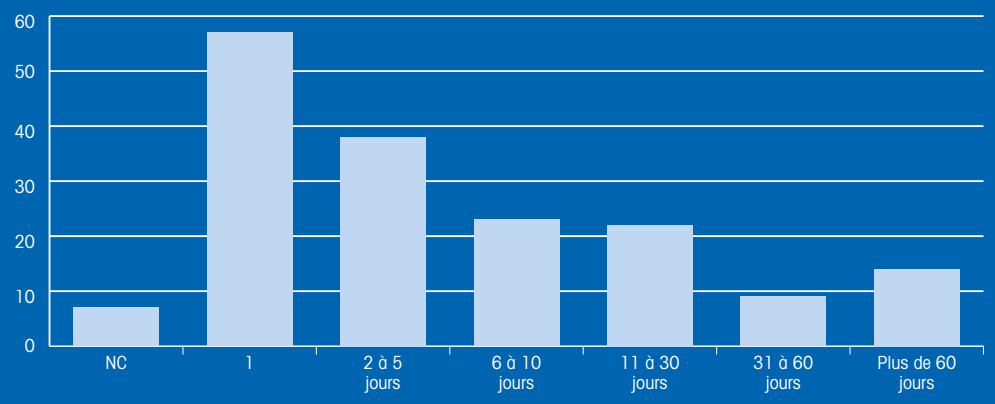
La CNPD attire également l'attention des responsables du traitement sur le fait qu'un certain nombre d'actes de piratage et de phishing sont ciblés sur le personnel de la direction d'une organisation et leur entourage (ex : assistant / secrétariat de la direction). Ces actes malveillants ont souvent comme objectif d'obtenir des informations permettant d'effectuer des transactions financières frauduleuses.

NOMBRE DE PERSONNES POTENTIELLEMENT IMPACTÉES PAR INCIDENT



(NC = nombre de personnes impactées par la violation non connu - cela peut être le cas lors d'une exfiltration de données à partir d'un système dont la journalisation des accès aux données à caractère personnel est mal adaptée ou inexistante)

NOMBRE DE JOURS ENTRE LE DÉBUT DE L'INCIDENT ET LA DÉTECTION DE L'INCIDENT



(NC = Date de début de l'incident non connue)

Plus de la moitié des incidents de sécurité sont détectés dans les 48 heures après de leur survenance. Toutefois, la CNPD a constaté que presque 18% des violations de données à caractère personnel ne sont détectées qu'au minimum un mois après s'être produites: il s'agit plus particulièrement d'incidents liés à des violations continues de la politique de sécurité de l'organisation (p.ex. : le personnel de direction envoie les données professionnelles sur leur email personnel pour travailler du domicile et l'email personnel est piraté), de données utilisées par des employés lors d'un départ d'une organisation et également de vol de données liée à des piratages non détectés.

La CNPD attire également l'attention des responsables du traitement sur le fait qu'un certain nombre d'actes de piratage et de phishing sont ciblés sur le personnel de la direction d'une organisation et leur entourage (ex : assistant / secrétariat de la direction). Ces actes malveillants ont souvent comme objectif d'obtenir des informations permettant d'effectuer des transactions financières frauduleuses.

Points d'attention identifiés :

1. La CNPD constate que de nombreuses organisations ont mis en place des procédures pour gérer et agir lorsqu'un incident sur des données à caractère personnel se produit. Toutefois, de nombreuses organisations sont moins matures en ce qui concerne la détection des incidents de sécurité.

2. La CNPD souhaite particulièrement attirer l'attention des organisations sur ce qu'elles ne doivent pas communiquer, dans les notifications, les données à caractère personnel concernées par la violation et les informations nominatives des personnes impliquées dans les violations de données.

3. Pour rappel, lorsqu'une organisation transmet une notification de violation à la CNPD, celle-ci accuse réception de la notification. La CNPD effectuera une communication ultérieure avec l'organisation qui notifie uniquement en cas de demande d'information complémentaire en rapport avec la notification. Dans le cadre du principe de responsabilisation (accountability), la CNPD intervient uniquement dans la gestion de la violation si elle l'estime nécessaire.

B) 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 2018, aucune violation de données dans le secteur des communications électroniques n'a été signalée à la CNPD.

2.4 DÉSIGNATION DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES

Depuis l'entrée en application du RGPD, les responsables du traitement et les sous-traitants doivent communiquer à la CNPD les coordonnées du délégué à la protection des données (DPD) qu'ils ont, le cas échéant, désigné.

Au 31 décembre 2018, 818 responsables du traitement ont communiqué les coordonnées de leur DPD à la CNPD. Au total, 493 personnes physiques ou morales ont été déclarés auprès de la CNPD.

Ce chiffre représente une augmentation importante par rapport à l'année 2017 où 150 personnes physiques ou morales étaient agréées pour exercer l'activité de chargé de la protection des données (sous l'ancien régime de la loi de 2002).

A ce titre, la CNPD a mis en ligne un formulaire de communication, ainsi qu'un site dédié qui répond aux questions fréquemment posées.

La désignation d'un DPD est obligatoire dans trois hypothèses :

- 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 ;
- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

A moins qu'il soit évident qu'un organisme n'est pas tenu de désigner un DPD, il est recommandé de documenter l'analyse interne effectuée afin de déterminer si, oui ou non, il y a lieu de désigner un DPD.

2.5 CONSULTATION PRÉALABLE DANS LE CADRE D'UNE ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Si un organisme a identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, il doit mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (Data Protection Impact Assessment ou DPIA).

L'analyse d'impact relative à la protection des données permet :
- d'élaborer un traitement de données personnelles ou un produit respectueux de la vie privée,
- d'apprécier les impacts sur la vie privée des personnes concernées,
- de démontrer que les principes fondamentaux du règlement sont respectés.

L'enjeu est d'apprécier les risques sur la protection des données du point de vue des personnes concernées.

Conformément à l'article 35.4 du RGPD, la CNPD a élaboré une liste de types d'opérations de traitement pour lesquels elle estime qu'une analyse d'impact sur la protection des données est obligatoire dans tous les cas. Il s'agit des types d'opérations suivants :

1. Les opérations de traitement portant sur des données génétiques telles que définies à l'article 4 (13) du RGPD, en combinaison avec au moins un autre critère figurant dans les lignes directrices du EDPB (European Data Protection Board), à l'exception des professionnels de santé qui fournissent des services de santé ;

2. Les opérations de traitement qui incluent des données biométriques telles que définies à l'article 4 (14) du RGPD aux fins d'identification des personnes concernées en combinaison avec au moins un autre critère des lignes directrices du EDPB ;

3. Les opérations de traitement impliquant la combinaison, la correspondance ou la comparaison de données à caractère personnel collectées à partir d'opérations de traitement ayant des finalités différentes (provenant du même ou de différents responsables du traitement) - à condition qu'elles produisent des effets juridiques à l'égard de la personne physique ou aient une incidence significative et similaire sur la personne physique ;

4. Les opérations de traitement qui consistent en ou qui comprennent un contrôle régulier et systématique des activités des employés - à condition qu'elles puissent produire des effets juridiques à l'égard des employés ou les affecter de manière aussi significative ;

5. Les opérations de traitement de fichiers susceptibles de contenir des données à caractère personnel de l'ensemble de la population nationale, à condition qu'une telle DPIA n'ait pas déjà été réalisée dans le cadre d'une analyse d'impact générale dans le contexte de l'adoption de cette base juridique ;

6. Les opérations de traitement à des fins de recherche scientifique ou historique ou à des fins statistiques au sens des articles 63 à 65 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données ;

7. Les opérations de traitement qui consistent en un suivi systématique de la localisation de personnes physiques ;

8. Les opérations de traitement reposant sur la collecte indirecte de données à caractère personnel en conjonction avec au moins un autre critère des lignes directrices du EDPB lorsqu'il n'est ni possible / ni réalisable de garantir le droit à l'information.

Il convient de souligner que la liste actuelle n'est pas une liste exhaustive de tous les types d'opération de traitement nécessitant la réalisation d'une DPIA. Ainsi l'absence d'un type d'opération de traitement sur cette liste ne signifie pas nécessairement qu'une DPIA n'est pas requise. La liste se limite aux activités de traitement qui nécessiteront toujours la réalisation d'une DPIA. Pour les activités de traitement ne figurant pas sur cette liste, les responsables du traitement des données devraient s'appuyer sur l'article 35 (1) du RGPD et sur les lignes directrices WP248 du groupe de travail de l'article 29 pour évaluer la nécessité d'une DPIA.

Si suite à l'analyse de risques sur les droits et libertés des personnes concernées de la DPIA il en résulte un (ou plusieurs) risque(s) résiduel(s) élevé si le responsable du traitement ne prenait pas de mesures pour l'atténuer, il doit consulter la CNPD qui va donner un avis sur le traitement envisagé.

Dans ce cas le traitement ne peut pas être mis en œuvre avant la réception de l'avis de la CNPD, et le cas échéant, la mise en œuvre des mesures supplémentaires.

En 2018, la CNPD n'a pas reçu de demande de consultation préalable respectant les critères tels que stipulés dans le RGPD.

La CNPD envisage d'effectuer dans les prochains mois une communication en rapport avec les DPIA afin de supporter les organisations dans leur mise en œuvre des analyses.

LES ACTIVITÉS EN 2018

3

2.6 CERTIFICATIONS

Les « certifications » représentent un nouvel outil pour les responsables de traitement et sous-traitants contribuant à démontrer que leurs opérations de traitement respectent le règlement général sur la protection des données (RGPD). Dans le cadre de nombreux échanges entre la CNPD et les entreprises pendant la phase de préparation au RGPD, celles-ci ont manifesté un intérêt particulier pour cette nouvelle possibilité.

La CNPD a été approchée par deux acteurs qui souhaitent soumettre leur projet de schéma de certification pour approbation.

Etant persuadée de la valeur ajoutée que la certification peut offrir, la CNPD a aussi pris une approche particulièrement proactive en élaborant, conjointement avec les professionnels du secteur, un schéma de certification.

Ainsi, le schéma dénommée « GDPR-CARPA » (GDPR - Certified Assurance Report based Processing Activities) a été soumis à une consultation publique en juin 2018.

La CNPD a orienté ses travaux selon deux piliers :

- Le premier pilier concerne les critères de certification auxquels doit répondre une organisation qui souhaite que certains de ses traitements de données soient certifiés. Ce pilier constituait une priorité dans le sens où une organisation candidate à la certification de ces traitements doit, le cas échéant, préalablement à la procédure de certification, mettre en place des mesures spécifiques pour pouvoir répondre favorablement aux critères. Les retours qui ont été fournis dans le cadre de la consultation publique ont permis à la CNPD de finaliser les travaux de ce pilier. Les organisations intéressées pour se faire certifier des traitements sont encouragées à étudier ces critères et d'évaluer dans quelle mesure elles veulent prendre une approche proactive pour se préparer. Les organisations intéressées peuvent s'adresser à la CNPD en cas de questions.

- Le deuxième pilier concerne les critères d'agrément auxquels doit répondre une organisation qui souhaite agir en tant qu'organisme de certification. Alors que le schéma de certification GDPR-CARPA, soumis à consultation publique reprenait déjà une description de ces critères, la CNPD a décidé de continuer à les développer, notamment pour les aligner avec les travaux d'élaboration d'une guidance sur les critères qui sont actuellement réalisés au niveau du European Data Protection Board (EDPB). L'objectif est d'assurer une cohérence européenne des travaux de la CNPD qui va communiquer ces critères à l'EDPB après finalisation de ladite guidance. La CNPD compte continuer à réaliser les travaux en concertation avec les professionnels du secteur disposant de compétences dans le domaine de la protection des données et dans le domaine de la certification.

2.7 TRANSFERTS INTERNATIONAUX DE DONNÉES PERSONNELLES

Les données à caractère personnel peuvent circuler librement depuis le Grand-Duché de Luxembourg au sein de l'Espace économique européen, tant que les principes généraux du RGPD sont respectés.

En effet, les États membres appliquent le même niveau de protection lors du traitement de données à caractère personnel. Un transfert au sein de l'Espace économique européen est régi de la même manière qu'un transfert au Luxembourg et doit par conséquent respecter les principes généraux du RGPD (respect notamment du principe de licéité, compatibilité de la communication avec le traitement d'origine, information des personnes concernées).

A) TRANSFERTS VERS UN PAYS EN DEHORS DE L'ESPACE ÉCONOMIQUE EUROPÉEN DISPOSANT D'UN NIVEAU DE PROTECTION ADÉQUAT

Tout responsable de traitement qui souhaite exporter des données à caractère personnel hors de l'Espace économique européen doit d'abord se renseigner sur le niveau de protection adéquat du pays destinataire. En effet, lorsque le pays tiers est considéré comme offrant un niveau de protection adéquat, le transfert peut être effectué comme s'il s'agissait d'un transfert au sein de l'Espace économique européen.

Le « EU-U.S. Privacy Shield Framework », ou sphère du bouclier de protection des données Union européenne – États-Unis, est un ensemble de principes de protection des données personnelles auxquelles les entreprises établies aux États-Unis d'Amérique sont libres d'adhérer.

Les entreprises établies dans l'Espace économique européen 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.

Les principes que ces sociétés américaines doivent respecter, négociés entre les autorités américaines et la Commission européenne en 2016, sont basés sur ceux de la directive européenne 95/46/CE sur la protection des données, et ont été réévalués en 2017 et 2018 sur base du règlement général sur la protection des données. Ils entendent par ailleurs répondre aux faiblesses du précédent accord dit « Safe Harbor », négociés en 2001 et invalidés par la Cour de justice de l'Union européenne en 2015.

B) TRANSFERTS VERS UN PAYS EN DEHORS DE L'ESPACE ÉCONOMIQUE EUROPÉEN NE DISPOSANT PAS D'UN NIVEAU DE PROTECTION ADÉQUAT

Pour les pays qui ne sont pas membre de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande) ou une organisation internationale vers laquelle les données sont transférées n'a pas été reconnue comme adéquate par la Commission européenne, il existe différentes possibilités pour un transfert de données.

Dans un tel cas, la CNPD recommande d'adopter, tout comme ses homologues européens, une approche par étapes fondée sur les meilleures pratiques et consistant à envisager de fournir des garanties adéquates. Les exportateurs de données devraient donc d'abord s'efforcer de trouver des possibilités de procéder au transfert à l'aide de garanties appropriées (clauses contractuelles, règles d'entreprise contraignantes (BCR), codes de conduite, mécanismes de certification ou garanties spécifiques pour le transfert entre autorités ou organismes publics), et ne recourir à des dérogations qu'en l'absence de telles garanties.

Les règles d'entreprise contraignantes

Les règles d'entreprise contraignantes (en anglais « binding corporate rules » ou BCR) permettent d'assurer un niveau de protection suffisant aux données transférées au sein d'un groupe d'entreprises tant à l'intérieur qu'à l'extérieur de l'Espace économique européen. Cette garantie appropriée se prête surtout aux groupe d'entreprises multinationales mettant en œuvre un grand nombre de transferts internationaux de données.

Les BCR constituent une « charte de la protection des données personnelles » élaborée par un groupe d'entreprises qui définit sa politique en matière de transferts de données à caractère personnel. Cette charte doit être contraignante et respectée par toutes les entités du groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs employés. En outre, elle doit conférer aux personnes concernées (clients, fournisseurs et/ou employés) des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel.

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

- conformité avec le règlement général sur la protection des données (article 47);
- limitation des garanties appropriées à mettre en œuvre pour chaque transfert (par exemple, l'adoption de BCR au niveau du groupe évite de devoir signer autant de clauses types de protection des données qu'il y a de transferts) ;
- uniformisation des pratiques relatives à la protection des données au sein d'un groupe ;
- guide interne en matière de protection des données personnelles, qui participe à la responsabilisation du groupe vis-à-vis du RGPD ;
- moyen plus flexible et adapté à la culture d'entreprise ;
- possibilité de placer la protection des données au rang de « préoccupation éthique du groupe ».

La procédure d'approbation des BCR s'opère en plusieurs étapes :

- identification de l'autorité de supervision principale (« lead authority »),
- procédure de coopération européenne entre l'autorité de supervision principale (« lead authority »), les autorités secondaires (« co-reviewers ») et les autres autorités concernées,
- avis (non contraignant) de l'EDPB au sujet du projet de décision consolidé soumis par l'autorité de supervision compétente,
- approbation (ou non) des BCR par l'autorité de supervision principale, en tenant compte de l'avis de l'EDPB.

En 2018, le groupe PayPal a adopté de nouvelles règles d'entreprises. Ce mécanisme se prête bien aux sociétés comme PayPal, mettant en œuvre un grand nombre de transferts internationaux de données. PayPal (Europe) S.à r.l. et Cie, S.C.A. est un établissement de crédit établi au Luxembourg et soumis à la surveillance de la CSSF (Commission de Surveillance du Secteur Financier). Sa société mère, PayPal Inc., est située en Californie aux États-Unis. Jusqu'en juillet 2015, l'entreprise faisait partie du groupe eBay, qui possède également une charte BCR validée par la CNPD. Suite à cette scission, PayPal a souhaité disposer de nouvelles règles d'entreprise contraignantes afin de maintenir un niveau élevé de protection des données quelle que soit leur localisation.

Depuis le départ par PayPal du groupe eBay, la CNPD a coopéré en qualité d'autorité chef de file (« lead authority ») avec ses homologues européens dans le cadre de la procédure de coopération et de reconnaissance mutuelle européenne. Suite à l'analyse effectuée par la CNPD, l'ensemble des autorités de protection des données européennes ont ainsi marqué leur accord pour autoriser au niveau national des transferts de données s'opérant dans le cadre de ces BCR.

2.8 MESURES CORRECTRICES ET SANCTIONS

En cas de traitement contraire à la règlementation en vigueur, la CNPD a le pouvoir d'adopter des mesures correctrices (p.ex. avertissement, rappel à l'ordre, limitation temporaire, limitation définitive, interdiction du traitement, amendes administratives, etc.).

En 2018, il y a lieu de distinguer entre deux périodes :

- la période du 01/01/2018 au 19/08/2018 pendant laquelle l'ancienne loi de 2002 sur la protection des données était encore applicable et
- la période du 20/08/2018 au 31/12/2018 pendant laquelle le RGPD et la nouvelle loi nationale de 2018 étaient applicables.

Période du 01/01/2018 au 19/08/2018

En vertu de l'article 33 de la loi de 2002, la CNPD pouvait prendre les sanctions disciplinaires suivantes :
- avertir ou admonester le responsable du traitement ayant violé les obligations relatives à la sécurité ;
- verrouiller, effacer ou détruire les données faisant l'objet d'un traitement contraire à la loi ;
- interdire temporairement ou définitivement un traitement contraire à la loi ;
- ordonner la publication d'une décision par la voie des journaux.

Pendant cette période, la CNPD a adopté 7 sanctions, à savoir 3 interdictions temporaires et 4 interdictions définitives de traitements de données contraires à la loi.

Période du 20/08/2018 au 31/12/2018

Sous le régime du RGPD et de la nouvelle loi de 2018, la CNPD a le pouvoir d'adopter des mesures correctrices et d'imposer des amendes administratives.

34 réclamations émises entre le 20/08/2018 et le 31/12/2018 ont fait l'objet de mesures correctrices, dont notamment :
- avertissement ou rappel à l'ordre ;
- demande de satisfaire aux requêtes présentées par la personne concernée en vue d'exercer ses droits ;
- demande de mise en conformité ou encore
- demande de rectification ou d'effacement de données à caractère personnel ou de limitation du traitement.

Les violations par le responsable du traitement du RGPD peuvent faire l'objet d'amendes pouvant s'élever jusqu'à vingt millions d'euros ou jusqu'à 4 % du chiffre d'affaire annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

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.

Rappelons que le législateur a choisi de limiter le pouvoir de la CNPD d'imposer des amendes administratives, dans la mesure où elle peut seulement infliger des amendes administratives à l'encontre de responsables du traitement issus du secteur privé, et non pas à l'encontre de l'État ou des communes.

Aucune amende n'a été imposée par la CNPD pendant les quatre mois suivant l'entrée en vigueur de la loi du 1er août 2018.

2.9 TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL EN MATIÈRE PÉNALE AINSI QU'EN MATIÈRE DE SÉCURITÉ NATIONALE

Conformément à l'article 10 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la CNPD établira un rapport annuel sur ses activités, qui comprend une liste des types de violations notifiées et des types de sanctions imposées en vertu de la loi du 1er août 2018 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.

2.10 RÉTENTION DE DONNÉES DE TRAFIC ET DE LOCALISATION

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

Or, la directive a été annulée par la Cour de justice de l'Union européenne en date du 8 avril 2014 par l'arrêt « Digital Rights Ireland ». Les lois de transposition nationales n'ont toutefois pas été modifiées en conséquence et la Commission nationale n'a pas reçu d'instruction dans ce cadre par son Ministère de tutelle. Elle continue à lui transmettre annuellement en vue de leur continuation à la Commission européenne des statistiques sur la conservation des données au titre des articles 5 et 9. À 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 2018, les autorités compétentes ont fait 4.766 demandes auprès des opérateurs. Ce chiffre a augmenté légèrement par rapport à l'année 2017 où 4.759 demandes avaient été faites. Sur les 4.766 demandes, 435 demandes n'ont pas pu être satisfaites.

3 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 2018 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). Ce groupe de travail a été remplacé par le Comité Européen de la Protection des Données (EDPB ou European Data Protection Board) à partir du 25 mai 2018.
- du « Groupe de Berlin », dédié à la protection des données dans le secteur des communications électroniques ;
- de la conférence de printemps des commissaires européens à la protection des données à Tirana ;
- de la conférence internationale des commissaires à la protection des données et de la vie privée à Bruxelles ;
- du séminaire européen « Case Handling Workshop » à Budapest.

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.

3.1 LE COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES

Le Comité Européen de la Protection des Données (EDPB – European Data Protection Board) est un organe européen indépendant qui contribue à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne et encourage la coopération entre autorités de l'UE chargées de la protection des données.

Il se compose de représentants des autorités nationales chargées de la protection des données et du Contrôleur européen de la protection des données (CEPD). L'EDPB est institué par le Règlement Général sur la Protection des Données (RGPD) et est basé à Bruxelles. La Commission européenne a le droit de prendre part aux activités et aux réunions du Comité, mais n'a pas le droit de vote.

L'EDPB dispose d'un secrétariat, qui est fourni par le CEPD. Un Protocole d'accord définit les conditions de la coopération entre l'EDPB et le CEPD.

L'EDPB a pour objectif de garantir l'application cohérente du Règlement Général sur la Protection des données ainsi que de la Directive Européenne en matière de Protection des Données dans le domaine répressif dans l'Union européenne.

Il peut adopter des documents d'orientation générale 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 RGPD lui confie également la mission d'adopter des décisions contraignantes envers les autorités de contrôle nationales afin de garantir une application cohérente de ses dispositions.

A) APPROBATION DES LIGNES DIRECTRICES DU GROUPE DE TRAVAIL « ARTICLE 29 »

Le 25 mai 2018, l'EDPB a remplacé le groupe de travail « Article 29 » (G29) et a approuvé des lignes directrices et documents de travail de son prédécesseur.

Il s'agit plus précisément des documents suivants :

1. Lignes directrices sur le consentement (WP 259)
2. Lignes directrices sur la transparence (WP 260)
3. Lignes directrices sur les décisions individuelles automatisées et le profilage (WP 251)
4. Lignes directrices sur les notifications de violations de données (WP 250)
5. Lignes directrices relatives au droit à la portabilité des données (WP 242)
6. Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » (WP 248)
7. Lignes directrices concernant les délégués à la protection des données (DPD) (WP 243)
8. Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant (WP 244)
9. Prise de position sur les dérogations à l'obligation de tenir un registre des activités de traitement conformément à l'article 30, paragraphe 5, du RGPD
10. Documents concernant les « règles d'entreprise contraignantes » (WP 263, WP 264, WP 265, WP 256, WP 257)
11. Critères de référence pour l'adéquation (WP 254)
12. Lignes directrices sur l'application et la fixation des amendes administratives aux fins du RGPD (WP 253)

B) LIGNES DIRECTRICES ADOPTÉES EN 2018

Lignes directrices 1/2018 sur la certification et l'identification des critères de certification conformément aux articles 42 et 43 du RGPD

Ces lignes directrices ont une portée limitée. Il ne s'agit pas d'un manuel de procédures pour la certification conformément au RGPD. L'objectif principal de ces lignes directrices est d'identifier les éléments suivants, les exigences et les critères qui peuvent s'appliquer à tous les types de mécanismes de certification délivrés conformément aux articles 42 et 43 du RGPD.

À cette fin, les lignes directrices :

- examinent la raison d'être de la certification en tant qu'outil de responsabilisation ;
- expliquent les concepts clés des dispositions des articles 42 et 43 relatives à la certification ; et
- expliquent la portée de ce qui peut être certifié en vertu des articles 42 et 43 et l'objet de cette certification ;
- contribuent à ce que le résultat de la certification soit significatif, sans ambiguïté, reproductible autant que possible et comparable, quel que soit le certificateur.

Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du RGPD

Ces orientations traitent des dérogations dans le contexte des transferts de données à caractère personnel vers des pays tiers.

Les dérogations visées à l'article 49 sont donc des exemptions du principe général selon lequel des données à caractère personnel ne peuvent être transférées vers des pays tiers que si un niveau de protection adéquat est offert dans le pays tiers ou si des garanties appropriées ont été apportées et si les personnes concernées bénéficient de droits opposables et effectifs afin de continuer à bénéficier de leurs droits fondamentaux et garanties. De ce fait et conformément aux principes de droit inhérents à l'ordre juridique européen, les dérogations doivent être interprétées de manière restrictive afin que l'exception ne devienne pas la règle. L'intitulé de l'article 49, qui indique que les dérogations doivent être utilisées pour les situations particulières (« Dérogations pour des situations particulières »), va aussi dans ce sens.

Dans ses lignes directrices, l'EDPB passe en revue les dérogations suivantes :

- la personne concernée a donné son consentement explicite au transfert envisagé ;
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;
- le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale ;

- le transfert est nécessaire pour des motifs importants d'intérêt public ;
- le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
- le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- transfert effectué au départ d'un registre public ;
- intérêts légitimes impérieux.

Lignes directrices 3/2018 sur le champ d'application territorial
L'EDPB a adopté un projet d'orientations qui favoriseront une interprétation commune du champ d'application territorial du RGPD et apporteront davantage de clarifications sur l'application du RGPD dans diverses situations, en particulier celles où le responsable du traitement ou le sous-traitant est établi hors de l'UE, notamment pour la désignation d'un représentant.

Les orientations font actuellement l'objet d'une consultation publique.

Lignes directrices 4/2018 sur l'agrément
L'EDPB a adopté une version révisée des lignes directrices du G29 relatives à l'agrément, y compris une nouvelle annexe. Le projet de lignes directrices avait initialement été adopté par le G29 et soumis à une consultation publique. L'EDPB a finalisé son analyse et est parvenu à une conclusion sur la version finale. L'objectif des lignes directrices est de fournir des orientations sur l'interprétation et la mise en œuvre des dispositions de l'article 43 du RGPD. Ces lignes directrices visent notamment à aider les États membres, les autorités de contrôle et les organismes nationaux d'accréditation à mettre en place des normes de référence cohérentes et harmonisées pour l'agrément des organismes de certification qui peuvent délivrer des certifications conformément au RGPD. Ces lignes directrices ont été complétées par une annexe, qui fournit des orientations concernant les exigences que les autorités de contrôle doivent imposer pour l'agrément des organismes de certification. Cette annexe a également fait l'objet d'une consultation publique.

C) DOCUMENTS DE TRAVAIL ET LETTRES

Lors de 5 réunions plénières en 2018, l'EDPB a adopté de nombreux documents de travail, guidances et lettres. Ces documents sont résumés ci-dessous et peuvent être téléchargés dans leur version complète sur Internet[4].

Directive DSP2
L'EDPB a adopté, au nom de sa présidente, une lettre adressée à Sophie in't Veld, députée européenne, concernant la directive révisée sur les services de paiement (directive DSP2). Dans sa réponse à Sophie in't Veld, l'EDPB a apporté un éclairage supplémentaire sur les « données des parties silencieuses » des fournisseurs tiers, les procédures concernant l'octroi et le retrait du consentement, les normes techniques de réglementation, la coopération

[4] https://edpb.europa.eu/our-work-tools/our-documents_fr

entre les banques et la Commission européenne, l'EDPB et le groupe de travail «Article 29» et ce qu'il reste à faire pour combler les lacunes persistantes en matière de protection des données.

Bouclier de protection des données

Judith Garber, l'ambassadrice et médiatrice américaine chargée du traitement des plaintes liées à la sécurité nationale au titre du bouclier de protection des données, a été invitée à la réunion plénière de l'EDPB pour un échange de vues avec les membres dudit Comité. Le Comité s'est montré particulièrement intéressé par les inquiétudes portées à la connaissance des États-Unis par son prédécesseur, le groupe de travail « Article 29 », concernant en particulier la nomination d'un médiateur permanent, les nominations officielles au Conseil de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board, PCLOB) et l'absence d'informations supplémentaires concernant le mécanisme du médiateur et la déclassification supplémentaire des règles procédurales, en particulier sur la manière dont le médiateur interagit avec les services de renseignement.

L'EDPB a souligné le fait que la réunion avec la médiatrice avait été intéressante et collégiale, mais n'avait apporté aucune réponse concluante aux dites inquiétudes et que ces questions resteraient au premier rang de ses priorités lors du deuxième examen annuel (programmé pour octobre 2018). En outre, il a demandé aux autorités américaines de lui fournir des éléments de preuve supplémentaires afin d'apaiser ces inquiétudes. Enfin, le Comité note que la Cour de justice de l'Union européenne fera part des mêmes préoccupations dans les affaires déjà en cours et pour lesquelles il proposera d'exprimer son point de vue, s'il y est invité par ladite Cour.

Décision d'adéquation UE-Japon

L'EDPB a adopté un avis portant sur le projet de décision d'adéquation UE-Japon, que la Commission européenne a soumis au comité en septembre 2018. L'EDPB a effectué son évaluation en se fondant sur les documents mis à disposition par la Commission européenne. L'objectif principal du EDPB était de déterminer si la Commission s'est assurée de l'existence de garanties suffisantes pour fournir un niveau adéquat de protection des données des personnes physiques dans le cadre japonais. Il est important de savoir que l'EDPB n'attend pas du cadre juridique japonais qu'il reproduise la législation européenne en matière de protection des données. L'EDPB se félicite des efforts consentis par la Commission européenne et par l'autorité japonaise chargée de la protection des données pour accroître la convergence entre les cadres juridiques japonais et européen. Les améliorations apportées par les règles complémentaires dans le but de réduire certaines différences entre les deux cadres juridiques sont très importantes, et sont accueillies avec satisfaction. Cependant, à l'issue d'une analyse minutieuse du projet de décision d'adéquation de la Commission et du cadre japonais de protection des données, l'EDPB note que certaines préoccupations subsistent, notamment en ce qui concerne la protection pour toute leur durée de vie des données à caractère personnel transférées de l'Union européenne vers le Japon. L'EDPB recommande à la Commission européenne de répondre à ses demandes de clarification, de fournir davantage d'éléments et d'explications concernant les questions soulevées, et de suivre de près l'application effective.

L'EDPB considère que la décision d'adéquation UE-Japon est de la plus haute importance. Cette décision constituera un précédent puisqu'il s'agit de la première décision d'adéquation depuis l'entrée en vigueur du Règlement général sur la protection des données (RGPD).

Listes relatives à l'AIPD
L'EDPB a adopté 26 avis établissant des critères communs applicables aux listes concernant l'analyse d'impact relative à la protection des données (AIPD).

Ces listes constituent un outil important pour l'application uniforme du RGPD dans l'ensemble de l'UE. L'AIPD est un processus permettant d'identifier et d'atténuer les risques relatifs à la protection de données qui pourraient affecter les droits et libertés des personnes. Afin de clarifier quel type de traitement nécessite une AIPD, le RGPD invite les autorités nationales de contrôle à créer et à publier des listes de types d'opérations susceptibles d'engendrer un risque élevé.

Ces listes contribueront à établir des critères communs au sein de l'EEE pour les analyses d'impact relatives à la protection des données.

Preuve électronique
L'EDPB a adopté un avis sur le nouveau règlement relatif aux preuves électroniques, proposé par la Commission européenne en avril 2018. Le comité a souligné que les nouvelles règles proposées pour la collecte des preuves électroniques devraient suffisamment préserver les droits des personnes en matière de protection des données et être plus cohérentes avec le droit de l'Union européenne sur la protection des données.

3.2 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 d'une réunion en 2018 à Budapest, le groupe a adopté des documents de travail sur :

- les véhicules connectés ;
- les standards en matière de protection des données concernant les demandes d'accès transfrontaliers à des fins pénales.

Ces documents peuvent être téléchargés dans leur intégralité (en anglais et en allemand) sur le site Internet du groupe de travail[5].

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

3.3 CONFÉRENCE DE PRINTEMPS DES AUTORITÉS EUROPÉENNES À LA PROTECTION DES DONNÉES

L'autorité de protection des données d'Albanie a organisé la « Spring conference » à Tirana les 3 et 4 mai 2018.

Les thèmes suivants ont notamment été abordés lors de la conférence intitulée « Data Protection : Better Together » :

- la coopération dans le domaine de la surveillance ;
- le champ d'application territorial du RGPD ;
- la modernisation de la Convention 108 ;
- la protection des données dans le domaine de la police et de la justice ;
- la protection des données dans le domaine de l'action humanitaire ;
- Cambridge Analytica et Facebook.

3.4 CONFÉRENCE INTERNATIONALE DES COMMISSAIRES DE LA PROTECTION DES DONNÉES

La CNPD a participé à la 40e conférence internationale des commissaires de la protection des données et de la vie privée organisée à Bruxelles du 22 au 26 octobre.

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.

La conférence a donné l'occasion aux commissaires de réfléchir ensemble sur la révolution numérique et son impact sur nos sociétés, ainsi que sur la façon dont une nouvelle éthique numérique pourrait contribuer à garantir le respect et la dignité dans notre monde dominé par la technologie.

Une déclaration sur la protection des données et l'éthique dans le domaine de l'intelligence artificielle a été adoptée.

Des résolutions relatives aux thèmes suivants ont été adoptées :

- les plateformes d'e-learning ;
- la modification des règles et procédures concernant la conférence internationale ;

- feuille de route sur l'avenir la conférence internationale ;
- la collaboration entre les autorités de protection des données et les autorités de protection des consommateurs ;
- le recensement concernant les conférences internationales.

3.5 LE SÉMINAIRE EUROPÉEN « CASE HANDLING WORKSHOP »

L'autorité de protection des données hongroise a organisé le séminaire européen « Case Handling Workshop » à Budapest du 27 au 29 novembre 2018.

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.

Les thèmes suivants ont été abordés au cours de 6 sessions :

- la vidéosurveillance : situation légale actuelle et jurisprudence ;
- traitement de données issues de registres publics ou de l'environnement en ligne ;
- transferts de données vers des pays tiers ;
- coopération entre autorités de protection des données de l'Union européenne et en dehors de l'Union européenne ;
- conditions pour exercer son droit d'accès ;
- assistance des PME dans la mise en conformité à la législation en matière de protection des données.

3.6 SIGNATURE DU PROTOCOLE D'AMENDEMENT DE LA CONVENTION 108 DU CONSEIL DE L'EUROPE

Le 10 octobre 2018, le Luxembourg a signé la protocole d'amendement à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108).

Ouverte à la signature le 28 janvier 1981, la « Convention 108 » du Conseil de l'Europe a été le premier instrument international juridiquement contraignant en la matière et a largement inspiré la législation adoptée par l'Union européenne.

Après plus de cinq années de négociations, cet instrument phare du Conseil de l'Europe a été modernisé.

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

1 RAPPORT DE GESTION RELATIF AUX COMPTES DE L'EXERCICE 2018

Dépenses

L'année 2018 a été marquée par l'entrée en application le 25 mai 2018 du nouveau règlement européen pour la protection des données (RGPD), qui marquera pour l'avenir la façon de fonctionner de la Commission nationale pour la protection des données (CNPD).

La préparation des acteurs concernés et impliqués à l'arrivée du RGPD a été la préoccupation majeure de tous les membres du personnel de la CNPD au cours de l'année 2018.

Si l'entrée en application du RGPD a également constitué autant de travail pour la CNPD du côté administratif que pour tout autre entité traitant des données personnelles en vue de sa propre mise en conformité, la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données a carrément donné une nouvelle base légale à la CNPD, lui permettant d'exécuter toutes les tâches et missions que le RGPD prévoit pour elle.

Certes, la CNPD telle qu'organisée par la nouvelle loi du 1er août 2018 a continué la personnalité juridique, y compris le personnel et les engagements juridiques de la Commission nationale pour la protection des données telle que créée par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard des traitements des données à caractère personnel aujourd'hui abrogée. Mais il y avait tout de même des ajustements à faire et des nouvelles structures à mettre en place, comme par exemple un Collège à quatre commissaires et un réviseur d'entreprises agréé. Les comptes de 2018 sont dès lors les premiers à être audités par un réviseur d'entreprises agréé.

Si le budget de la CNPD pour 2017 était un budget annonçant le changement, le budget pour l'année 2018 était un budget de transformation vers une CNPD capable d'assumer les tâches et missions lui octroyées par le RGPD. En effet, le budget de 2018 présentait une augmentation de 85% par rapport à l'année précédente, avec un passage de 2.386.726 € à 4.415.419 € de dotation autorisée.

Tout comme l'année précédente, les fonds supplémentaires étaient essentiellement destinés au recrutement d'effectifs additionnels 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 2018 s'élevaient à 3.604.308,93 € ce qui constitue une augmentation de 42,37% par rapport à l'exercice précédent qui s'élevait à 2.531.584,32 €.

Le total des frais de fonctionnement reste toutefois en dessous du montant des prévisions budgétaires originaires estimées à 4.435.519 €.

La différence de 831.214,07 € s'explique essentiellement par deux positions, à savoir les dépenses pour charges relatives au personnel, d'autre part, par les frais pour la gestion et la maintenance des systèmes et réseaux.

En effet, pour ce qui est des charges relatives au personnel permanent et temporaire, celles-ci ont certes augmenté sensiblement, pour atteindre 3.106.940,50 € en 2018 comparés à 2.257.695,91 € en 2017. Les dépenses réelles restent tout de même 17,43% en dessous des prévisions budgétaires estimées à 3.648.592 €. Ce résultat est dû au fait que tous les recrutements nécessaires n'ont pas été effectués en début d'année, alors que la CNPD voulait attendre pour voir quel était l'évolution réelle de la charge de travail escomptée. Alors qu'en début de l'année, la charge de travail à venir était difficilement appréciable, elle se cristallisait de façon d'autant plus forte aux alentours de l'entrée en application du RGPD le 25 mai 2018 et plus particulièrement du lancement du système de coopération européen. C'est uniquement à partir de ce moment-là que la CNPD avait une vue claire sur les profils nécessaires pour le renforcement de son personnel. S'y ajoutait l'adoption tardive de la nouvelle loi d'organisation de la CNPD, qui prévoyait entre autres un 4e commissaire, dont le recrutement ne s'est pas réalisé en 2018. Et c'est seulement avec l'adoption de la loi de transposition de la Directive (UE) 2016/68, que la CNPD a pu évaluer plus concrètement ses besoins en personnel dans le cadre de la surveillance en matière pénale ainsi qu'en matière de sécurité nationale. Une fois les profils exacts définis, la recherche de candidats appropriés s'est avérée également difficile.

La CNPD a néanmoins engagé à plein temps et à durée indéterminée un employé de la carrière B1, un employé de la carrière A2 et 10 employés de la carrière A1. Dans la même période, 2 employés B1 engagés à durée déterminée ont cessé leurs fonctions et le statut de quatre employés de la carrière A1 ont été convertis en celui de fonctionnaire suite à la réussite de l'examen-concours par les candidats en question.

A noter qu'un fonctionnaire de la carrière B1 continue à bénéficier d'un congé pour travail à mi-temps pour des raisons médicales et qu'un autre est absent depuis 10 mois. Alors que la CNPD ne peut pas profiter de la provision globale de l'État pour remplacements, elle assume elle-même les frais pour ces absences.

Pour ce qui est des charges pour la gestion et la maintenance des systèmes et réseaux, la CNPD pressentait que ses rôles et responsabilités allaient fortement évoluer avec l'arrivée du RGPD. Afin de pouvoir assurer ses responsabilités de manière efficiente, la mise en place d'une informatisation poussée et systématique des procédures de travail existantes et futures est devenue nécessaire. Pour soulever les défis et assurer un service efficace de haute qualité, la CNPD avait opté pour une digitalisation poussée. Dans cette perspective, la CNPD avait réorienté le modèle

opérationnel de son service informatique pour qu'il utilise les évolutions technologiques des dernières années comme levier pour assurer une augmentation soutenable de l'efficacité, de la qualité et de la transparence de son activité. Ainsi, la CNPD fait depuis 2018 recours à un service de type Plateforme As A Service (Cloud), dont le prestataire est le CTIE. Selon le prix du marché, le service offert équivaudrait à 308.240,07 €. En 2018, la facture ne s'élevait toutefois qu'à 55.803,15 €. Cette différence s'explique par le fait que la CNPD a pu développer sa nouvelle plateforme de travail « SharePoint » en utilisant exclusivement des composants standards du CTIE. De ce fait, le système de la CNPD peut être opéré sur une plateforme standard et mutualisé du CTIE – réduisant fortement les coûts. Un montant de 66.988,35 € a par ailleurs été déboursé pour l'hébergement de l'outil « CNPD Compliance Support Tool », développé par la CNPD ensemble avec le LIST (Luxembourg Institute of Science and Technology) par une société spécialisée.

Concernant les frais d'honoraires, un montant de 46.000 € avait été prévu pour couvrir les frais de la fiduciaire, les frais pour le personnel de remplacement et une provision pour honoraires juridiques. Les frais de la fiduciaire, qui tient la comptabilité et établit le bilan de l'établissement public, sont restés légèrement en dessous des prévisions avec 17.048,52 € par rapport aux 19.000 € prévus. Il n'y a pas eu de dépenses, ni pour personnel de remplacement, ni à titre d'honoraires d'avocats. Par contre, dans le cadre de l'élaboration de ses procédures d'audit – une des nouvelles missions clés, la CNPD a fait recours à une société de consultance spécialisée. Les coûts engagés pour cette prestation s'élevaient à 56.890,08 €. Le total de cette position s'élevait donc à 73.938,60 € et dépassaient donc de 60,73 % les prévisions.

Le montant des charges locatives pour le bâtiment administratif à Belval s'élevait à 14.981,37 €, montant légèrement supérieur au montant de l'année précédente qui s'élevait à 12.262,33 €, mais en dessous des prévisions sur cette position, qui avaient été estimées à 30.000 €, alors qu'elle couvre les frais de nettoyage pour l'annexe louée auprès du Fonds Belval. Or, en raison d'un déménagement tardif, les frais étaient moins élevés que prévus.

Les frais de port et de télécommunications ont connu une baisse, alors que depuis le 25 mai 2018, la CNPD n'émet plus d'autorisations et n'accuse plus réception de notifications et par conséquent, envoie beaucoup moins de lettres, ce qui a résulté en une baisse des frais d'affranchissement. Les 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 significativement alors que la CNPD a dû équiper les nouveaux collaborateurs, voire les bureaux sis à l'annexe louée auprès du Fonds Belval. Les frais y relatifs figurent au tableau d'amortissement.

Les frais de déplacement et de séjour à l'étranger se chiffraient à 48.826,77 € ce qui s'explique par le nombre élevé de réunions auxquelles les membres du personnel de la CNPD ont dû participer en amont de

l'entrée en application du RGPD. A l'avenir, ce montant n'a pas vocation à baisser. Au contraire, alors qu'une des pierres angulaires du RGPD est la coopération européenne qui nécessite un échange permanant et dense entre les autorités de contrôle européennes. Les engagements de la CNPD à l'étranger ne feront qu'augmenter au futur, alors que non seulement le nombre de groupes de travail que la CNPD doit couvrir à l'étranger a tendance à augmenter. La cadence des réunions du nouveau Comité européen pour la protection des données affiche également une progression substantielle par rapport aux réunions de son prédécesseur, le Groupe de travail de l'Article 29. La forte augmentation sur cette position par rapport aux chiffres de l'année précédente où le montant s'élevait à 29.255,66 €, nette baisse encore par rapport à 2016 où cette même dépense s'élevait à 39.529,20 €, en dehors de réunions préparatoires à l'entrée en vigueur du RGPD, s'explique aussi par un changement peu favorable des horaires de train, qui ne permet plus aux membres du personnel de la CNPD d'être à l'heure aux réunions à Bruxelles à moins de se lever très tôt le même jour. Il s'ensuit que les collaborateurs se rendent à Bruxelles la veille des réunions ce qui engendre des coûts supplémentaires pour l'hébergement.

Les frais de formation externe hors frais de déplacement et de séjour pour le personnel ont fortement augmenté pour atteindre 26.209,30 € en 2018, comparés à 9.282,43 en 2017, voir 3.440,80 € en 2016, ce qui dépasse de 37,79% les 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 avait 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 102.699,41 € en 2018, par rapport à 23.846,85 € en 2017. Bien que ce montant dépassait de plus de 37.000 € les prévisions budgétaires de 65.000 €, cette dépense est hautement justifiée alors que l'entrée en application du RGPD constituait un événement qui nécessitait un maximum d'information et de sensibilisation de tous les acteurs impliqués. La CNPD a ainsi continué la réalisation et l'impression de nouvelles brochures de sensibilisation et a organisé un nombre d'événements de sensibilisation ouverts au public.

Les amortissements comptabilisés en 2018 atteignaient un montant total de 16.111,56 €, c'est-à-dire une somme nettement supérieure au montant de l'année précédente qui était de 6.888,22 €. Cette augmentation est essentiellement due d'une part au développement de logiciels informatiques pour un montant total de 12.583,35 € et d'autre part, à l'acquisition de nouveau mobilier destiné à accueillir les nouveaux membres du personnel de la CNPD en 2018 pour un montant total de 42.743,61 €.

Recettes

Jusqu'au 25 mai 2018, la CNPD émettait des autorisations et recevait des notifications conformément aux dispositions de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Le montant des redevances perçues en application des articles 37 paragraphe (4), 13 paragraphe (3) et 14 paragraphe (4) de cette loi s'élevait à 48.495,00 € comparé à 178.318,51 € en 2017. Bien que le montant est inférieur à celui de l'année précédente, il est tout de même supérieur aux prévisions budgétaires qui ne prévoient qu'une recette de 20.100,00 €. En prévision de l'entrée en application du RGPD, la CNPD était confrontée à un afflux des formalités préalables et par conséquent, d'une augmentation correspondante des recettes, qui ont toutefois disparus depuis lors. Aucune recette de produits financiers (intérêts créditeurs) n'a pu être enregistrée pour l'année 2018.

Résultat d'exploitation

Compte tenu de la dotation annuelle de 4.415.419 €, dont la Commission nationale a bénéficié en 2018 de la part de l'État en application de l'article 37 paragraphe (4) de la loi du 2 août 2002 précitée, le résultat d'exploitation de l'établissement public s'élève à 859.605,07 € au 31 décembre 2018.

2 PERSONNEL ET SERVICES

Collège
Tine A. LARSEN, présidente
Thierry LALLEMANG, commissaire
Christophe BUSCHMANN, commissaire

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

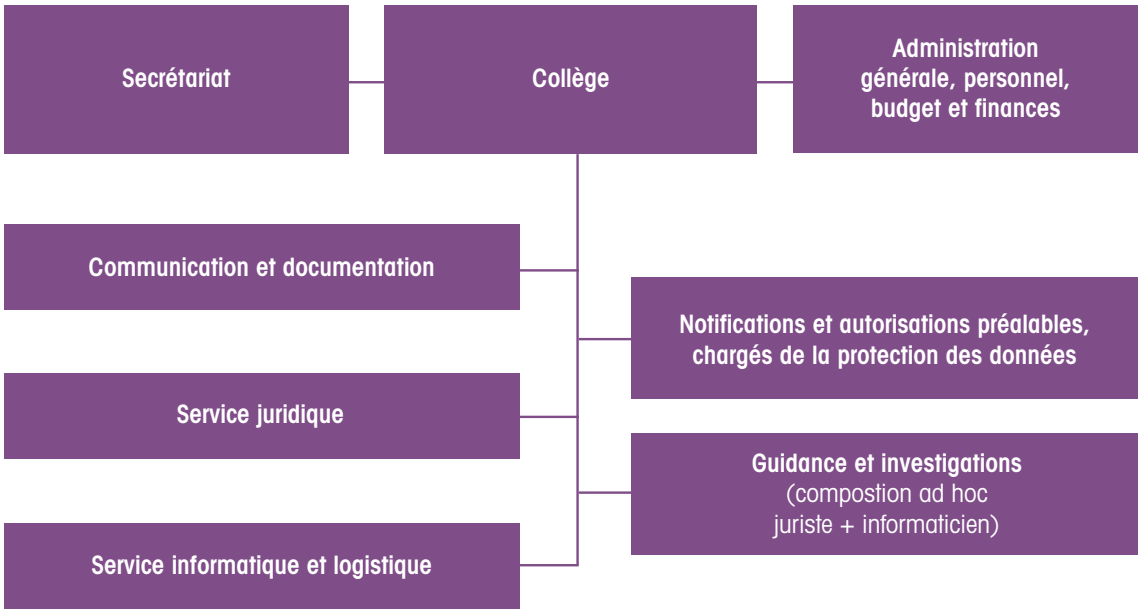
Secrétariat, administration générale, ressources humaines, budget, finances, IT et logistique
Irena ADROVIC, attachée
Jan KUFFER, employé de l'État
Anna MAGI, employée de l'État
Stéphanie MATHIEU, rédacteur
Tessy PATER, rédacteur
Maryse WINANDY, employée de l'État

Service communication et documentation
Tom KAYSER, attaché

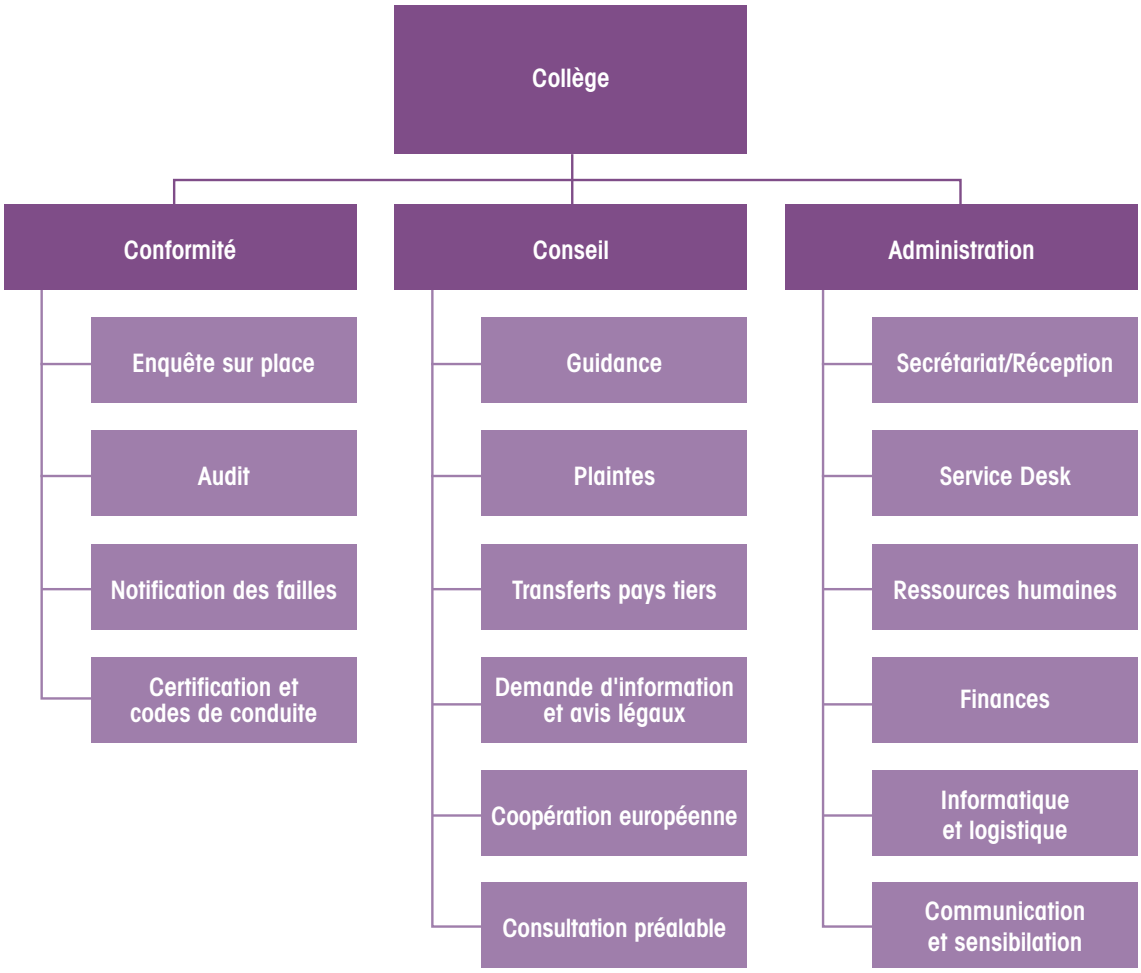
Service opérationnel
Clémentine BOULANGER, employée de l'État
Marie-Laure FABBRI, employée de l'État
Arnaud HABRAN, employé de l'État
Alain HERRMANN, chargé d'études
Danielle JEITZ, attachée
Alexandre KUHN, employé de l'État
Vincent LEGELEUX, chargé d'études
Laurent MAGNUS, employé de l'État
Edith MALHIERE, employée de l'État
Francis MAQUIL, attaché
Marc MOSTERT, rédacteur
Bertrand NAVARRE, employé de l'État
Claudia PFISTER, employée de l'État
Nicolas RASE, employé de l'État
Mathieu RINCK, employé de l'État
Carmen Schanck, attachée
Romy SCHAUS, attachée
Céline SIMON-HERTZ, employée de l'État
Michel SINNER, conseiller
Mathilde STENERSEN, attachée
Sébastien TEISSEIRE, employé de l'État
Georges WEILAND, conseiller
Christian WELTER, conseiller

3 ORGANIGRAMME DE LA CNPD

3.1 ORGANIGRAMME DU 01.01.2018 AU 24.05.2018



3.2 ORGANIGRAMME DU 25.05.2018 AU 31.12.2018



ANNEXES

5

5 ANNEXES

AVIS ET DÉCISIONS

- Deuxième 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 10 novembre 2009 relative aux services de paiement ; 6. de la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif ; 7. de la loi modifiée du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs ; 8. de la loi modifiée du 7 décembre 2015 sur le secteur des assurances ; 9. de la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement ; et 10. de la loi du 23 décembre 2016 relative aux abus de marché
  (Délibération n° 1/2018 du 9 janvier 2018) 86

- Avis relatif au projet de loi n° 7128 portant 1. transposition des dispositions ayant trait aux obligations professionnelles et aux pouvoirs des **autorités de contrôle en matière de lutte contre le blanchiment et contre le financement du terrorisme** de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission; 2. mise en œuvre du règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006 ; 3. modification de: a) la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ; b) la loi modifiée du 10 novembre 2009 relative aux services de paiement ; c) la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat ; d) la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice ; e) la loi modifiée du 10 août 1991

sur la profession d'avocat ; f) la loi modifiée du 5 avril 1993 relative au secteur financier ; g) la loi modifiée du 10 juin 1999 portant organisation de la profession d'expert-comptable ; h) la loi du 21 décembre 2012 relative à l'activité de Family Office ; i) la loi modifiée du 7 décembre 2015 sur le secteur des assurances ; j) la loi du 23 juillet 2016 relative à la profession de l'audit
(Délibération n° 51/2018 du 18 janvier 2018) 89

- Avis complémentaire de la Commission nationale pour la protection des données à l'égard du projet de loi n° 7113 relatif au **Revenu d'inclusion sociale**
(Délibération n° 59/2018 du 23 janvier 2018) 104

- Avis à l'égard de l'avant-projet de règlement grand-ducal relatif à l'organisation et les méthodes de travail du **service national de coordination des dons d'organes**
(Délibération n° 79/2018 du 31 janvier 2018) 108

- Avis relatif au projet de règlement grand-ducal relatif à la **radioprotection**
(Délibération n° 138/2018 du 23 février 2018) 114

- Avis relatif au projet de règlement grand-ducal portant fixation des **indemnités revenant au Président, aux membres et aux membres suppléants de la Commission nationale** pour la protection des données et abrogeant le règlement grand-ducal du 7 juillet 2003
(Délibération n° 139/2018 du 1er mars 2018) 117

- Avis relatif au projet de règlement grand-ducal portant fixation du **siège de la Commission nationale pour la protection des données** et abrogeant le règlement grand-ducal du 7 juillet 2003 portant transfert du siège de la Commission nationale pour la protection des données
(Délibération n° 140/2018 du 1er mars 2018) 119

- Avis à l'égard du projet de loi relative à des **mesures macroprudentielles portant sur les crédits immobiliers résidentiels** et portant modification de la loi modifiée du 5 avril 1993 relative au secteur financier, et de la loi du 1er avril 2015 portant création d'un comité du risque systémique et modifiant la

ANNEXES

5

loi modifiée du 23 décembre 1998 relative au statut monétaire et à la Banque centrale du Luxembourg
(Délibération n° 220/2018 du 29 mars 2018) 121

- Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal précisant les **modalités et conditions de mise en place du dossier de soins partagé**
(Délibération n° 242/2018 du 5 avril 2018) 124

- Avis complémentaire relatif au projet de règlement grand-ducal pris en exécution de la loi du 5 juillet 2016 portant **réorganisation du Service de renseignement de l'État**
(Délibération n° 244/2018 du 12 avril 2018) 149

- Avis complémentaire relatif aux amendements gouvernementaux 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'État 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° 279 /2018 du 25 avril 2018) 158

- Avis relatif au projet de loi n° 7248 relatif au **financement des travaux d'extension et de perfectionnement du Réseau national intégré de radiocommunication pour les services de sécurité et de secours luxembourgeois** et portant modification de la loi du 20 mai 2014 relative au financement du Réseau national intégré de radiocommunication pour les services de sécurité et de secours luxembourgeois
(Délibération n° 283/2018 du 27 avril 2018) 165

- Deuxième avis complémentaire relatif aux amendements parlementaires au projet de loi n° 7184 portant **organisation de la Commission nationale pour la protection des données et 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 et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État
(Délibération n° 423/2018 du 8 juin 2018) 171

- Avis relatif au projet de règlement grand-ducal concernant : 1. la **vente par internet au public de médicaments à usage humain**; 2. la préparation, la division, le conditionnement ou le reconditionnement des médicaments à usage humain.
(Délibération n° 440/2018 du 9 juillet 2018) 179

- Avis relatif au projet de loi n° 6539 relatif à la préservation des entreprises et portant **modernisation du droit de la faillite**
(Délibération n° 441/2018 du 16 juillet 2018) 183

- Avis relatif au projet de loi n° 7287 portant **organisation de la cellule de renseignement financier** (CRF) et modifiant : 1. le Code de procédure pénale ; 2. la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ; 3. la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme
(Délibération n° 442/2018 du 16 juillet 2018) 186

- Deuxième avis complémentaire relatif au projet de règlement grand-ducal pris en exécution de la loi du 5 juillet 2016 portant **réorganisation du Service de renseignement de l'État**
(Délibération n° 443/2018 du 16 juillet 2018) 191

- Avis relatif au projet de loi n° 6961 portant 1. **création de l'Autorité nationale de sécurité** et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2) du Code pénal
(Délibération n° 444/2018 du 16 juillet 2018) 193

ANNEXES

5

- Avis relatif au projet de loi n° 7269 complétant le Code du travail en portant **création d'une activité d'assistance à l'inclusion dans l'emploi pour les salariés handicapés et les salariés en reclassement externe**
  (Délibération n° 445/2018 du 16 juillet 2018) 198

- Avis à l'égard de l'avant-projet de règlement grand-ducal portant modification 1° de l'arrêté grand-ducal modifié du 23 novembre 1955 portant règlement de la **circulation sur toutes les voies publiques**, 2° du règlement grand-ducal modifié du 26 janvier 2016 sur le **contrôle technique des véhicules routiers** et 3° du règlement grand-ducal modifié du 26 janvier 2016 relatif à la **réception et l'immatriculation des véhicules routiers**
  (Délibération n° 449/2018 du 16 juillet 2018) 201

- Avis à l'égard du projet de loi n° 7258 portant modification 1) de la loi modifiée du 25 février 1979 concernant **l'aide au logement**, 2) de la loi modifiée du 21 septembre 2006 sur le bail à usage d'habitation et modifiant certaines dispositions du Code civil, et 3) de la loi modifiée du 16 décembre 2008 concernant l'accueil et l'intégration des étrangers au Grand-Duché de Luxembourg, et à l'égard du règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14quater-1 et 14quater-2 de la loi modifiée du 25 février 1979 concernant l'aide au logement
  (Délibération n° 450/2018 du 14 septembre 2018) 208

- Avis relatif au projet de règlement grand-ducal déterminant le **contenu minimal du dossier individuel du patient hospitalier et du résumé clinique de sortie**
  (Délibération n° 481/2018 du 19 octobre 2018) 212

- Avis relatif au projet de loi n° 7217 instituant un Registre des bénéficiaires effectifs et portant 1° transposition des dispositions de l'article 30 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la **prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme**, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen

et du Conseil et la directive 2006/70/CE de la Commission, telle que modifiée par la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018; 2° modification de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises et au projet de règlement grand-ducal portant exécution de la loi du 13/01/2019 instituant un Registre des bénéficiaires effectifs
(Délibération n° 486/2018 du 22 novembre 2018) 218

- Avis relatif au projet de règlement grand-ducal portant exécution de la loi du 1er août 2018 sur la **déclaration obligatoire de certaines maladies** et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire
(Délibération n° 489/2018 du 7 décembre 2018) 229

- Avis à l'égard du projet de loi n° 7126 relative aux **sanctions administratives communales** modifiant 1) le Code pénal, 2) le Code de procédure pénale, et 3) la loi communale modifiée du 13 décembre 1988
(Délibération n° 490/2018 du 7 décembre 2018) 240

- Avis relatif au projet de règlement grand-ducal précisant les modalités de gestion de l'identification des personnes et les catégories de données contenues dans les **annuaires référentiels d'identification des patients et des prestataires**
(Délibération n° 491/2018 du 21 décembre 2018) 243

Deuxième avis complémentaire de la Commission nationale pour la protection des données 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 10 novembre 2009 relative aux services de paiement ; 6. de la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif ; 7. de la loi modifiée du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs ; 8. de la loi modifiée du 7 décembre 2015 sur le secteur des assurances ; 9. de la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement ; et 10. de la loi du 23 décembre 2016 relative aux abus de marché

Délibération n° 1/2018 du 9 janvier 2018

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 » ou « 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 ».*

Le 8 janvier 2018, la Commission des Finances et du Budget a proposé des amendements 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 (ci-après désigné « le projet de loi »). Au vu des changements apportés par les amendements 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 les amendements parlementaires.

La CNPD a rendu un premier avis relatif au projet de loi n° 7024 le 16 mars 2017 (délibération n° 243/2017) et un avis complémentaire le 27 juillet 2017 (délibération n° 654/2017). Dans ces avis, la CNPD a rappelé que les professionnels du secteur financier et du secteur des assurances devront structurer leurs projets de sous-

traitance de façon à respecter non seulement la législation spécifique à leur secteur, 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, à savoir le règlement (UE) 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 « RGPD »), 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. Par ailleurs, la Commission nationale a 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.

Concernant les amendements sous avis, la CNPD prend acte du nouveau paragraphe (9) de l'article 41 de la loi modifiée du 5 avril 1993, du nouveau paragraphe (12) de l'article 30 de la loi modifiée du 10 novembre 2009 relative aux services de paiement et du nouveau paragraphe (11) de l'article 300 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, qui précisent chaque fois que *« le présent article est sans préjudice de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ».*

Elle salue l'ajout de ces paragraphes, qui clarifient les textes en questions en énonçant de manière explicite et dans le corps même des textes que la règlementation actuelle et future en matière de protection des données s'applique à toutes les relations de sous-traitance qui impliquent le traitement de données à caractère personnel. Notons dans ce contexte que le RGPD, applicable à partir du 25 mai 2018, constituera une norme supérieure à la loi en projet sous avis.

La CNPD note à cet égard qu'en vertu de l'article 60 du 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 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'État 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, la référence à la loi du 2 août 2002 sera remplacée par une référence au RGPD.

Tant la Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, qui a été transposée en droit luxembourgeois par la loi modifiée du 2 août 2002, que le nouveau règlement européen visent à faciliter la libre circulation des données au sein de l'Union en harmonisant les règles européennes relatives à la protection des données[1]. Les transferts de données à caractère personnel vers d'autres États membres de l'Union européenne dans

[1] Voir l'article 1er de la Directive 95/46/EC et l'article 1er du règlement (UE) 2016/679.

le cadre d'une sous-traitance seront dès lors encadrés par un cadre juridique uniforme garantissant la protection des données à caractère personnel. En ce qui concerne le recours à un prestataire de service situé dans un pays tiers, la CNPD rappelle que les transferts de données à caractère personnel vers des pays tiers doivent être effectués dans le respect des conditions énoncées dans la loi modifiée du 2 août 2002 et dans le RGPD, qui s'ajouteront aux obligations prévues par les dispositions du présent projet de loi.

Ainsi décidé à Esch-sur-Alzette en date du 9 janvier 2018.

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 n° 7128 portant 1. transposition des dispositions ayant trait aux obligations professionnelles et aux pouvoirs des autorités de contrôle en matière de lutte contre le blanchiment et contre le financement du terrorisme de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission; 2. mise en oeuvre du règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006 ; 3. modification de: a) la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ; b) la loi modifiée du 10 novembre 2009 relative aux services de paiement ; c) la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat ; d) la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice ; e) la loi modifiée du 10 août 1991 sur la profession d'avocat ; f) la loi modifiée du 5 avril 1993 relative au secteur financier ; g) la loi modifiée du 10 juin 1999 portant organisation de la profession d'expert-comptable ; h) la loi du 21 décembre 2012 relative à l'activité de Family Office ; i) la loi modifiée du 7 décembre 2015 sur le secteur des assurances ; j) la loi du 23 juillet 2016 relative à la profession de l'audit

Délibération n° 51/2018 du 18 janvier 2018

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 ».

Par courrier en date du 8 mai 2017, Monsieur le Ministre des Finances a invité la Commission nationale à se prononcer sur le projet de loi portant transposition des dispositions ayant trait aux obligations professionnelles et aux pouvoirs des autorités de contrôle en matière de lutte contre le blanchiment et contre le financement du terrorisme

de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (ci-après « le projet de loi »)[2].

Le projet de loi a pour objectif de modifier la législation luxembourgeoise actuelle, notamment la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (ci-après désignée « la loi modifiée du 12 novembre 2004 » ou « la loi de 2004 »), afin de la rendre conforme aux nouvelles règles européennes, et plus particulièrement la Directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (ci-après désignée « la Directive 2015/849 »). Certains aspects de cette Directive et du projet de loi impliquent la collecte, l'analyse, la conservation et le partage de données à caractère personnel d'une multitude de personnes concernées tant par les professionnels tombant dans le champ d'application de la loi modifiée du 12 novembre 2004 (ci-après désignés « les professionnels »), que par les autorités chargées de la surveillance des professionnels[3]. Les auteurs du projet de loi doivent dès lors veiller au respect de la règlementation en matière de la protection des données lors de la transposition de la Directive 2015/849.

La CNPD relève 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.

Les législateurs européens ont adopté, en parallèle avec le RGPD, la Directive (UE) 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 désignée « la Directive Police et Justice »). La Directive Police et Justice doit être transposée en droit interne au plus tard le 6 mai 2018 et *« établit des règles relatives 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »*[4].

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 de la nouvelle législation européenne d'autre part. De façon générale, vu la matière en cause, la CNPD recommande de tenir compte des changements apportés par les deux mesures

[2] Ce projet de loi tend également à :
- mettre en œuvre le règlement (UE) 2015/ 847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006 ; et
- modifier : a) la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat ; b) la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice ; c) la loi modifiée du 10 août 1991 sur la profession d'avocat ; d) la loi modifiée du 5 avril 1993 relative au secteur financier ; e) la loi modifiée du 10 juin 1999 portant organisation de la profession d'expert-comptable ; f) la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme ; g) la loi modifiée du 10 novembre 2009 relative aux services de paiement ; h) la loi du 21 décembre 2012 relative à l'activité de Family Office ; i) la loi modifiée du 7 décembre 2015 sur le secteur des assurances ; j) la loi du 23 juillet 2016 relative à la profession de l'audit.

[3] Directive 2015/849, considérant 43.

[4] Directive Police et Justice, article 1er, paragraphe (1).

législatives précitées, dans la mesure du possible, notamment comme certains des traitements mis en œuvre sur base du projet de loi tomberaient dans le champ d'application de la loi transposant la Directive 2016/680, respectivement le projet de loi n° 7168[5].

En tenant compte de l'envergure du projet de loi, la Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de loi sous examen, qui justifient une analyse à cause des risques pour les personnes concernées ou à cause des changements apportés par le RGPD et la Directive Police et Justice.

I. Quant au champ d'application de loi modifiée du 2 août 2002, le RGPD et la Directive Police et Justice

La Commission nationale note la transposition littérale de l'article 41 de la Directive (UE) 2015/849 par l'article 6, point 10 du projet de loi. Cet article, qui introduit l'article 3, paragraphe (6bis) à la loi modifiée du 12 novembre 2004, énonce que *« le traitement de données à caractère personnel en vertu de la présente loi est soumis à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel, dénommée ci-après « loi modifiée du 2 août 2002 » »*. Comme il est d'ailleurs déjà le cas, la loi de 2002 s'appliquerait aux traitements effectués par les professionnels, les autorités et par la Cellule de Renseignement Financier (ci-après « la CRF »).

Comme soulevé ci-avant, la loi de 2002 sera remplacée par le RGPD à partir du 25 mai 2018. Les traitements effectués par la CRF dans le cadre de ses missions en matière de lutte contre le blanchiment ne tomberont cependant pas dans le champ d'application du RGPD, mais dans celui de la Directive Police et Justice. En effet, en application de l'article 2, paragraphe (1) du projet de loi n° 7168, *« la présente loi s'applique au traitement de données à caractère personnel effectué par les autorités compétentes aux fins énoncées à l'article 1er. Elle s'applique également aux traitements qui sont effectués en exécution : … (c) des missions de la Cellule de Renseignement Financier ».*

La CNPD attire encore l'attention des auteurs du projet de loi sur le considérant (11) de la Directive Police et Justice, qui traite du chevauchement potentiel des deux champs d'application de ladite Directive et du RGPD, en notant que : *« Par conséquent, le règlement (UE) 2016/679 s'applique lorsqu'un organisme ou une entité recueille des données à caractère personnel à d'autres fins et les traite ultérieurement pour respecter une obligation légale à laquelle il est soumis. Par exemple, les établissements financiers conservent, à des fins de détection ou de poursuites d'infractions pénales ou d'enquêtes en la matière, certaines données à caractère personnel qu'ils traitent et qu'ils ne transmettent aux autorités nationales compétentes que dans des cas spécifiques et conformément au droit des États membres. Un organisme ou une entité qui traite des données à caractère personnel pour le compte de ces autorités dans le cadre du champ d'application de la présente directive devrait être lié par un contrat ou un autre acte juridique et par les dispositions applicables aux sous-traitants en vertu de la présente directive, le règlement (UE) 2016/679 continuant de s'appliquer aux traitements de données à caractère personnel par le sous-traitant en dehors du champ d'application de la présente directive ».*

[5] Projet de loi n° 7168 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.

II. Quant à la finalité des traitements

Tant la loi modifiée du 2 août 2002 que le RGPD consacrent le principe de limitation des finalités, selon lequel les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités[6].

L'article 41, paragraphe (2) de la Directive 2015/849 définit explicitement la finalité des traitements mis en œuvre sur base du projet de loi en précisant que *« les données à caractère personnel ne sont traitées sur la base de la présente directive par des entités assujetties qu'aux fins de la prévention du blanchiment de capitaux et du financement du terrorisme, au sens de l'article 1er, et ne font pas l'objet d'un traitement ultérieur d'une manière incompatible avec lesdites finalités. Le traitement des données à caractère personnel sur la base de la présente directive pour toute autre finalité, par exemple à des fins commerciales, est interdit. »* Le projet de loi, en transposant cette disposition, omet la référence à l'interdiction de traiter des données à des « fins commerciales ». En effet, selon l'article 6, point 10, alinéa 2 du projet de loi, *« Les données à caractère personnel ne sont traitées sur la base de la présente loi par des professionnels qu'aux fins de la prévention du blanchiment et du financement du terrorisme et ne font pas l'objet d'un traitement ultérieur d'une manière incompatible avec lesdites finalités. Le traitement des données à caractère personnel sur la base de la présente loi pour toute autre finalité est interdit ».*

Comme le recueil des données traitées aux fins de la lutte contre le blanchiment et contre le terrorisme s'effectue en parallèle avec la collecte des données traitées à des fins commerciales, il est essentiel de délimiter avec précision la finalité des traitements des données collectées dans le cadre du présent projet de loi. Dès lors, et dans un souci de transposition correcte de la Directive 2015/849 en droit national, la CNPD estime nécessaire de reprendre littéralement le libellé de la Directive 2015/849, afin d'indiquer explicitement que le traitement des données à des fins commerciales n'est pas compatible avec les fins de la prévention du blanchiment de capitaux et du financement du terrorisme.

III. Quant aux données traitées

Le chapitre 2 de la loi modifiée du 12 novembre 2004 aborde la question des obligations des professionnels. Plus particulièrement, en application des articles 3 à 3-2 de la prédite loi, tels que modifiés par le projet de loi, les professionnels doivent soumettre tous leurs clients à un contrôle rigoureux afin de satisfaire à leurs obligations de vigilance. Les professionnels peuvent déterminer l'étendue des mesures appliquées en fonction de leur appréciation du risque[7]. Le projet de loi ne précise cependant pas les données à caractère personnel du client qui devraient ou peuvent être collectées afin de remplir les obligations imposées par les dispositions en question.

Par exemple, dans le cadre de l'identification du bénéficiaire de fiducies, de trusts ou de constructions juridiques similaires, l'article 6, point 5 du projet de loi, qui insère un paragraphe (2quater) à l'article 2 de la loi de 2004,

[6] Loi modifiée du 2 août 2002, article 4, paragraphe (1), lettre (a) et RGPD, article 5, paragraphe (1), lettre (b).

impose aux professionnels l'obligation de recueillir *« suffisamment d'informations sur le bénéficiaire pour se donner l'assurance d'être à même de pouvoir identifier le bénéficiaire au moment du versement des prestations ou au moment où le bénéficiaire exerce ses droits acquis ».*

Des imprécisions quant aux données qui devraient être traitées par les professionnels pourraient résulter dans une collecte indifférenciée des données non-pertinentes des clients par les professionnels[8]. Or, comme soulevé par le Conseil d'État à l'occasion du projet de loi n° 5165, qui introduisait la loi modifiée du 12 novembre 2004, *« la lutte antiblanchiment et antiterrorisme ne doit pas conduire au „gläserner Mensch". Sans rentrer ici dans le débat, longuement mené par d'autres avis, au sujet de la collision entre le projet sous avis et la loi du 2 août 2002 relative à la protection des personnes à l'égard des traitements de données à caractère personnel, le Conseil d'État retient que la poursuite justifiée d'un pourcentage infime de criminels ne doit pas porter des atteintes démesurées à la vie privée, constitutionnellement protégée »*[9].

La CNPD rappelle à cet égard l'article 4, paragraphe (1), lettre (b) de la loi de 2002 et l'article 5, paragraphe (1), lettre (c) du RGPD, selon lesquelles seules les données pertinentes et nécessaires au regard des finalités poursuivies par le responsable du traitement doivent être collectées.

La CNPD rappelle encore que le traitement des catégories particulières de données[10] ainsi que le traitement des données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté pourraient engendrer des risques importants pour les personnes concernées et sont dès lors soumis à des cadres juridiques plus contraignants[11]. Par exemple, l'article 8 de la loi modifiée du 2 août 2002 et l'article 10 du RGPD prohibent le traitement des données relatives aux condamnations pénales, aux infractions, et aux mesures de sûreté, sauf si le traitement est effectué sous le contrôle de l'autorité publique ou si une disposition légale prévoit un tel traitement.

Alors que le projet de loi ne prévoit pas explicitement que les professionnels devraient traiter de telles données, il ne peut être exclu qu'ils seront amenés à les traiter lors de l'accomplissement de leurs obligations de vigilance.

Vu ce qui précède, afin d'empêcher une collecte indifférencié de données par les professionnels et dans un souci de sécurité juridique, la CNPD recommande, à l'instar de la recommandation du CEPD émise dans son avis sur le projet de Directive n° 2015/849, d'amender le projet de loi afin d'indiquer dans un seul texte légal ou règlementaire les catégories de données, y compris, le cas échéant, les catégories particulières de données ou les données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté, qui doivent être prises en compte pour l'application des obligations de vigilance à l'égard de la clientèle[12]. Les autorités de contrôles pourraient, le cas échéant, adopter ou amender des règlements énumérant les données à un stade ultérieur, afin de tenir compte des besoins spécifiques des différentes catégories de professionnels.

[7] Projet de loi n° 7128, article 6, point 3.
[8] Avis du Contrôleur européen de la protection des données du 4 juillet 2013, op.cit., point 73.
[9] Avis du Conseil d'État relatif au projet de loi n° 5165 relative à la lutte contre le blanchiment et contre le financement du terrorisme portant transposition de la directive 2001/97/CE du Parlement européen et du Conseil du 4 décembre 2001 modifiant la directive 91/308/CEE du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux, doc. parl. 5165/5, p. 5.
[10] Loi modifiée du 2 août 2002, article 6 et RGPD, article 9.
[11] RGPD, considérant 51.
[12] Avis du Contrôleur européen de la protection des données du 4 juillet 2013, op.cit., points 75 et 79.

IV. Quant aux personnes politiquement exposées

En vertu de l'article 3-2, paragraphe (4) de la loi de 2004, pour le cas où un client serait à considérer comme une personne politiquement exposée (ci-après « la PPE »), les professionnels seraient tenus d'appliquer des mesures de vigilance renforcées. En application de l'article 1er, paragraphe (9) de la loi modifiée du 12 novembre 2004, tel qu'il résulte du projet de loi, sont considérées comme des personnes politiquement exposées, *« des personnes physiques qui occupent ou se sont vu confier une fonction publique importante, ainsi que les membres de leur famille ou des personnes connues pour leur être étroitement associées ».*

Il résulte de l'article 3, paragraphe (10) de la Directive 2015/849 que *« les membres de la famille »* de la personne physique qui occupe ou s'est vu confier une fonction publique importante sont : son conjoint, ou une personne considérée comme l'équivalent d'un conjoint, ses enfants et leurs conjoints ou des personnes considérées comme l'équivalent d'un conjoint, et ses parents. En transposant cette disposition, les auteurs du projet de loi ont ajouté les « frères et sœurs » à la définition de « membres de la famille » figurant au paragraphe (11) de l'article 1er de la loi de 2004, tel que modifié par le projet de loi, afin d'aligner *« la définition des « membres de la famille » à celle prévue dans les lignes directrices émises par le GAFI»*[13].

En application de cette modification par les auteurs du projet de loi, les professionnels devraient ainsi appliquer un contrôle minutieux des données à caractère personnel relatives aux frères et sœurs de la personne physique qui occupe ou s'est vu confier une fonction publique importante. Or, cette modification étend le champ d'application au-delà de ce qui a été jugé nécessaire lors de la rédaction de la Directive 2015/849. Afin de limiter le cercle des personnes soumises automatiquement à des mesures de vigilance renforcées, la CNPD recommande que les auteurs du projet de loi reprennent la définition exacte de *« membres de la famille »*, telle qu'elle figure dans la Directive 2015/849.

V. Quant au traitement des données relatives aux salariés

Il ressort de l'article 4, paragraphe (1), lettre (a) de la loi de 2004, tel qu'il résulte du projet de loi, que les professionnels doivent mettre en place des politiques, contrôles et procédures internes relatifs à *« la sélection du personnel »*.

Tout comme la Chambre de Commerce[14], la CNPD s'interroge sur l'étendue de cette obligation. S'agit-il d'un contrôle au début de la relation de travail ou d'un contrôle continu ? Alors que *« la sélection du personnel »* semble se référer au début de la relation de travail, la version anglaise de la Directive 2015/849 parle d'*« employee screening »*, qui semble indiquer qu'il s'agit d'un contrôle continu. Or, ni les articles, ni le commentaire des articles indiquent la périodicité du contrôle des salariés.

[13] Projet de loi n° 7128, doc. parl. n° 7128/00, Commentaire des articles, p. 43.
[14] Avis de la Chambre de Commerce relatif au projet de loi n° 7128, doc. parl. n° 7128/01, page 22.

En tout état de cause, la CNPD soulève que l'article 4, paragraphe (4) du 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 concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ». Dans la mesure où le contrôle de la sélection du personnel pourrait constituer une évaluation de la fiabilité ou le comportement du salarié, que ce soit au début ou lors de la relation du travail, un contrôle de la sélection du personnel pourrait constituer un profilage au sens du RGPD.

La CNPD rappelle encore que seules les données pertinentes et nécessaires au regard des finalités poursuivies par le responsable du traitement doivent être collectées[15]. Or, la disposition dans sa version actuelle ne précise pas quelles données devraient, le cas échéant, être traitées dans le cadre de la sélection du personnel.

Etant donné que le contrôle des salariés pourrait être qualifié de « profilage » au sens de l'article 4, paragraphe (4) du RGPD et afin de limiter l'ingérence dans la vie privée des salariés par les professionnels, la CNPD estime nécessaire de préciser dans le projet de loi l'étendue de ce contrôle, y compris une indication des données qui devraient être traitées. Elle rappelle en outre à cet égard les recommandations récemment émises par le Groupe de travail « Article 29 » relatives aux traitements de données sur le lieu de travail et notamment les sections relatives au « screening » des candidats et des salariés[16].

VI. Quant à l'information et l'accès aux données à caractère personnel

a. L'information

En vertu du nouvel alinéa 3 de l'article 3, paragraphe (2bis) de la loi modifiée du 12 novembre 2004, qui transpose l'article 41, paragraphe (3) de la Directive 2015/849, « les professionnels communiquent aux nouveaux clients les informations requises en vertu de l'article 26, paragraphe (1), de la loi modifiée du 2 août 2002 avant de nouer une relation d'affaires ou d'exécuter une transaction à titre occasionnel. Ces informations contiennent en particulier un avertissement général concernant les obligations légales des professionnels au titre de la présente loi en ce qui concerne le traitement des données à caractère personnel aux fins de la prévention du blanchiment et du financement du terrorisme ».

La CNPD rappelle que l'article 13 du RGPD, qui remplacera l'article 26, paragraphe (1) de la loi modifiée du 2 août 2002, étend la liste des informations obligatoires que le responsable du traitement devra fournir aux personnes concernées.

b. Le droit d'accès

Selon l'article 28 de la loi modifiée du 2 août 2002, les personnes concernées disposent d'un droit d'accès

[15] Loi modifiée du 2 août 2002, article 4, paragraphe (1), lettre (b) et RGPD, article 5, paragraphe (1), lettre (c).
[16] Avis 02/2017 du Groupe de travail « Article 29 » du 8 juin 2017 relatif aux traitements de données sur le lieu de travail (WP 249).

aux données les concernant, afin de s'assurer notamment de leur exactitude et de la licéité de leur traitement[17]. Les exceptions au droit d'accès sont notamment prévues à l'article 29 de la loi de 2002, en vertu duquel les responsables du traitement sont autorisés à limiter ou différer le droit d'accès dans certains cas, par exemple, si le traitement est nécessaire pour sauvegarder *« la prévention, la recherche, la constatation ou la poursuite d'infractions pénales, y compris celles à la lutte contre le blanchiment, … »*[18].

Le RGPD encadre le droit d'accès dans l'article 15 et prévoit, dans son article 23, que le droit de l'Union ou le droit d'un État Membre peut limiter ce droit dans certains cas, comme, par exemple pour *« d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale »*[19]. La mesure législative prévoyant la limitation doit être assortie des dispositions spécifiques qui circonscrivent la limitation du droit, comme, par exemple, des dispositions relatives à l'étendue des limitations introduites[20] et aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites[21].

Selon le considérant 46 la Directive 2015/849, *« l'accès de la personne concernée aux informations liées à une déclaration de transaction suspecte nuirait gravement à l'efficacité de la lutte contre le blanchiment de capitaux et le financement du terrorisme »*. Dès lors, afin de ne pas compromettre l'efficacité des mesures prévues par la règlementation en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, l'article 6, point 10, alinéa 4 du projet de loi, qui transpose l'article 41, paragraphe (4) de la Directive 2015/849, énonce :

« En application de l'article 29, paragraphe (1), lettre (d), de la loi modifiée du 2 août 2002, le responsable de traitement limite ou diffère l'exercice du droit d'accès de la personne concernée aux données à caractère personnel la concernant lorsqu'une telle mesure est nécessaire pour :

a) permettre au professionnel, à la cellule de renseignement financier, à une autorité de contrôle ou à un organisme d'autorégulation d'accomplir ses tâches comme il convient aux fins de la présente loi ou des mesures prises pour son exécution ; ou
b) éviter de faire obstacle aux demandes de renseignements, analyses, enquêtes ou procédures à caractère officiel ou judiciaire, menées aux fins de la présente loi, des mesures prises pour son exécution ou de la directive (UE) 2015/849 et pour ne pas compromettre la prévention et la détection des cas de blanchiment ou de financement du terrorisme ni les enquêtes en la matière. ».

La CNPD tient à remarquer que selon l'article 29, paragraphe (4) de la loi modifiée du 2 août 2002, un responsable du traitement, qui limite le droit d'accès, doit indiquer le motif de la limitation. Par ailleurs, dans un tel cas, la personne concernée dispose d'un droit d'accès indirect par le biais de la CNPD, qui pourra informer la personne concernée du résultat de ses investigations, sans toutefois mettre en danger la ou les finalités des traitements en question[22]. Le considérant 46 de la Directive 2015/849 évoque cet accès indirect en indiquant que *« la personne*

[17] Directive 95/46/CE, considérant 41.
[18] Loi modifiée du 2 août 2002, article 29, paragraphe (1), lettre (d).
[19] RGPD, article 23, paragraphe (1), lettre (e).
[20] RGPD, article 23, paragraphe (2), lettre (c).
[21] RGPD, article 23, paragraphe (2), lettre (d).
[22] Loi modifiée du 2 août 2002, article 29, paragraphe (5).

concernée a le droit de demander qu'une autorité de contrôle visée à l'article 28 de la directive 95/46/CE ou, le cas échéant, le Contrôleur européen de la protection des données vérifie la licéité du traitement et a le droit de former le recours juridictionnel visé à l'article 22 de ladite directive. … Sans préjudice des restrictions au droit d'accès, l'autorité de contrôle devrait être en mesure d'informer la personne concernée que toutes les vérifications nécessaires ont été effectuées par l'autorité de contrôle et du résultat en ce qui concerne la licéité du traitement en question. »

En tenant compte de ce qui précède et vu les nouvelles exigences du RGPD, le projet de loi devrait stipuler des garanties pour les personnes concernées, notamment que celles-ci puissent exercer leur droit d'accès aux données les concernant indirectement auprès de la Commission nationale pour la protection de données (par exemple, selon les modalités prévues au paragraphe (5) de l'article 29 de la loi modifiée du 2 août 2002).

VII. Quant à la durée de conservation

La Commission nationale rappelle qu'en application de l'article 4, paragraphe (1), lettre (d) de la loi modifiée du 2 août 2002 et de l'article 5, paragraphe (1), lettre (e) du RGPD, les données traitées doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. La durée de conservation des données à caractère personnel étant ainsi un des principes fondamentaux relatifs au traitement de données à caractère personnel et doit dès lors figurer dans la loi.

Afin de satisfaire à ce principe[23], la Directive 2015/849 fixe la durée de conservation des documents tenus par les professionnels à cinq ans après la fin de la relation d'affaires ou de la transaction conclue à titre occasionnel, cette durée étant la durée minimale recommandée par le GAFI[24]. Elle prescrit ensuite dans son article 40 que les données doivent être effacées à l'issue de la période de conservation, sauf *« dispositions contraires du droit national, lequel précise dans quelles circonstances les entités assujetties peuvent ou doivent prolonger la conservation des données »*.

Le projet de loi reprend ces exigences dans son article 6, point 9, en précisant qu'elles s'appliquent également aux informations relatives aux mesures qui ont été prises pour identifier les bénéficiaires économiques[25].

Pour ce qui est de la fixation de la durée de conservation, la Directive 2015/849 accorde aux États membres une certaine marge de manouvre dans la détermination de celle-ci dans la mesure où ils peuvent prolonger la durée de conservation pour une durée ne dépassant pas cinq années supplémentaires, *« après avoir minutieusement évalué la nécessité et la proportionnalité de cette conservation prolongée et si elle a été jugée nécessaire aux fins de prévenir ou de détecter des actes de blanchiment de capitaux ou de financement du terrorisme ou d'enquêter en la matière »*. La prolongation de la durée de conservation est dès lors clairement soumise à une analyse approfondie de la nécessité de la mesure.

[23] Directive 2015/849, considérant 44.
[24] *Ibidem.*
[25] Loi modifiée du 12 novembre 2004, article 3, paragraphe (6), 4eme alinéa, tel qu'introduit par le projet de loi n° 7148, article 6, point 9.

Or, selon l'article 6, point 9 du projet de loi, les professionnels pourraient de leur propre initiative prolonger la durée de conservation de cinq ans, lorsque cela serait *« nécessaire pour la mise en œuvre efficace des mesures internes de prévention ou de détection des actes de blanchiment de capitaux ou de financement du terrorisme »*[26]. Le commentaire des articles justifie cette faculté en observant que les *« informations sur le comportement historique d'un client et des personnes avec lesquelles il conclut régulièrement des transactions constituent des éléments essentiels dans l'appréciation des risques de blanchiment ou de financement du terrorisme émanant d'une transaction ou d'une relation d'affaires particulière »*[27].

La CNPD estime que cette formulation générale n'est pas conforme avec la précision dans la Directive 2015/849 qu'une prolongation de la durée de conservation doit être fondée sur une analyse approfondie de la nécessité et proportionnalité de la prolongation. Bien que la précision faite dans le commentaire des articles puisse démontrer la nécessité de prolonger la durée de conservation, les auteurs du projet de loi n'ont pas procédé à une analyse de la proportionnalité de la mesure.

Par ailleurs, la formulation imprécise qui permettrait aux professionnels de prolonger la durée de conservation de cinq ans après la fin de la durée de conservation initiale, si une telle prolongation serait nécessaire *« pour la mise en œuvre efficace des mesures internes »*, ne limite pas suffisamment les cas dans lesquels les professionnels pourraient procéder à une telle prolongation et pourrait dès lors conduire à ce que la dérogation devienne la règle et qu'une multitude de professionnels conserveraient les données au-delà du délai de cinq ans instauré par la Directive 2015/849.

Vu ce qui précède, la CNPD estime nécessaire que les auteurs du projet de loi indiquent des précisions quant à la proportionnalité de cette dérogation. Par ailleurs, pour le cas où cette option serait maintenue, la disposition devrait davantage préciser les cas restrictifs dans lesquels les professionnels pourraient prolonger la durée de conservation.

Ces remarques sont également valables pour les modifications apportées à la loi modifiée du 10 novembre 2009 relative aux services de paiement[28].

VIII. Quant aux transferts des données à caractère personnel

Il ressort du futur article 4-1, paragraphe (1) de la loi de 2004, qui serait inséré par l'article 11 du projet de loi sous examen, que les professionnels qui font partie d'un groupe multinational doivent mettre en œuvre des politiques et procédures efficaces, notamment des politiques de protection des données, au niveau des succursales et filiales détenues majoritairement et établies dans des États membres et dans des pays tiers.

La Commission nationale relève que les mécanismes visés aux articles 18 et 19 de la loi modifiée du 2 août 2002, ou à compter du 25 mai 2018, aux articles 44 à 49 du RGPD, devront être mises en œuvre par le responsable

[26] Loi modifiée du 12 novembre 2004, article 3, paragraphe (6), 5ème alinéa, tel qu'introduit par le projet de loi n° 7148, article 6, point 9.
[27] Projet de loi n° 7128, doc. parl. n° 7128/00, Commentaire des articles, p. 46.
[28] Voir l'article 58-4 de la loi modifiée du 10 novembre 2009 relative aux services de paiement, tel qu'ajouté par le projet de loi n° 7128.

du traitement lorsque celui-ci transfère des données à caractère personnel vers des pays tiers. Il peut s'agir par exemple, en ce qui concerne les transferts vers des pays tiers n'assurant pas un niveau adéquat de protection des données, de clauses types de protection des données ou de règles d'entreprises contraignantes.

IX. Quant aux traitements effectués par les autorités de contrôle et les organismes d'autorégulation

Comme soulevé plus haut, les autorités et la CRF sont soumises aux règles en matière de protection des données découlant de la loi de 2002 à l'heure actuelle, et, à partir de 2018, des règles du RGPD (projet de loi n° 7184), respectivement ceux de la loi transposant la Directive Police et Justice (projet de loi n° 7168).

a. L'Administration de l'enregistrement et des domaines

i. Les finalités des traitements effectués par l'AED

Le nouvel article 8-2, paragraphe (4) de la loi modifiée du 12 novembre 2004 introduit les traitements qui pourraient être effectués par l'AED. Selon l'alinéa 1er dudit paragraphe, *« les pouvoirs de l'AED visés au paragraphe (1), alinéa 1, incluent le droit de recourir à l'ensemble des bases de données dont elle est le responsable de traitement et de s'entourer de toutes les informations requises en vue d'apprécier si un professionnel respecte les obligations professionnelles qui lui incombent en vertu de la présente loi.*

Aux fins de l'alinéa 1, l'AED dispose d'un accès au registre du commerce et des sociétés.

Le ministre ayant l'Economie dans ses attributions transmettra mensuellement à l'AED un relevé des professionnels disposant d'une autorisation d'établissement et qui sont soumis au pouvoir de surveillance de l'AED conformément à l'article 2-1, paragraphe (8) ». Par opposition aux deux premiers traitements, la finalité de cette transmission n'est pas indiquée dans le texte.

Le commentaire des articles précise que la finalité des trois traitements effectués sur base du paragraphe (4), à savoir l'utilisation ultérieure de ses bases de données, l'accès au RCS et la transmission du relevé, consisterait dans la seule identification des professionnels *(« Le paragraphe 4 trouve sa source dans le besoin de l'identification par l'AED des professionnels dont elle a la surveillance »)*[29]. Les finalités des traitements ne sont dès lors pas clairement déterminées dans le texte en projet.

Or, s'agissant d'une matière réservée à la loi, les points essentiels, dans le cas d'espèce les finalités des traitements, doivent figurer dans la loi[30]. Par ailleurs, comme l'a déjà soulevé le Conseil d'État à plusieurs reprises *« …l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, est une matière réservée à la loi formelle »*[31].

[29] Projet de loi n° 7128, doc. parl. n° 7128/00, commentaire des articles, p. 51.

[30] Voir l'article 32, paragraphe (3) de la Constitution et l'avis du Conseil d'État du 14 juillet 2017 relatif au projet de loi 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, doc. parl. n° 7024/08, p. 4.

[31] Avis du Conseil d'État du 7 juin 2016 concernant le projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'État pour études supérieures, doc. parl. n° 6975/5, p. 4. Voir aussi l'avis du Conseil d'État du 9 décembre 2014 à l'égard du projet de loi 6588 portant organisation du secteur des services de taxis et modification du code de la consommation, doc. parl. n° 6588/8, p. 7.

Pour le cas où la finalité des deux premiers traitements identifiés dans le paragraphe (4), à savoir l'utilisation des données figurant dans les bases de données et l'accès au RCS, consisterait dans la surveillance du respect des obligations professionnelles découlant de la loi par les professionnels et que la finalité du troisième traitement, à savoir la transmission du relevé des professionnels par le ministre ayant l'Économie dans ses attributions, consisterait dans l'identification des professionnels, ceci doit résulter clairement du texte de la loi. Il conviendrait dès lors de suivre l'ordre chronologie des traitements afin d'améliorer la lisibilité du paragraphe, en prévoyant en premier le ou les traitements effectué(s) pour identifier les professionnels et puis les traitements mis en œuvre aux fins de la surveillance des professionnels par l'AED.

ii. Les données à caractère personnel traitées par l'AED

La CNPD s'interroge encore sur les données qui pourraient être traitées par l'AED. Plus particulièrement, pour ce qui est du relevé transmis par le ministre ayant l'Économie dans ses attributions, le projet de loi ne précise pas le contenu, respectivement quelles données figureraient sur le relevé. A cet égard, la Commission nationale renvoie à l'arrêt *« Smaranda Bara »* de la Cour de Justice de l'Union européenne (ci-après désignée « CJUE ») du 1er octobre 2015, dans lequel la CJUE a retenu que *« les articles 10, 11 et 13 de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, doivent être interprétés en ce sens qu'ils s'opposent à des mesures nationales, telles que celles en cause au principal, qui permettent à une administration publique d'un État membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement »*[32].

Afin que la transmission puisse se faire dans le plein respect de la règlementation en matière de protection des données à caractère personnel, il convient dès lors d'adapter le projet de loi afin d'y indiquer de façon limitative les données figurant sur le relevé.

Pour ce qui est de l'utilisation de *« toutes les bases de données dont elle est le responsable du traitement »*, la CNPD est à se demander quelles bases de données et quelles données y contenues seraient exploitées, vu que ni le texte du projet de loi sous avis, ni le commentaire des articles ne les énumère.

La CNPD tient à rappeler qu'en application de l'article 4, paragraphe (1), lettre (b) de la loi modifiée du 2 août 2002 et de l'article 5, paragraphe (1), lettre (c) du RGPD, seules les données pertinentes et nécessaires au regard des finalités poursuivies par le responsable du traitement doivent être collectées. En l'absence de précision quant aux bases de données concernées et des données y traitées, la CNPD ne pourra pas se prononcer sur la légalité, la nécessité ou la proportionnalité d'une telle utilisation et elle doit insister sur l'indication précise des bases de données et des données auxquelles l'AED pourrait avoir recours.

[32] Arrêt du 1er octobre 2015, Smaranda Bara et autres, C 201/14, EU:C:2015:638, point 46.

La CNPD s'interroge encore sur la formulation de la disposition sous examen selon laquelle l'AED pourrait *« recourir à l'ensemble des bases de données dont elle est le responsable du traitement et s'entourer de toutes les informations requises »*. S'agit-il d'autres données que celles contenues dans ses bases de données? Le commentaire des articles reste vague à ce sujet en indiquant que *« l'AED devra s'entourer non seulement des bases de données dont elle dispose en interne. … Vu que ces bases de données ne sont pas suffisantes pour pouvoir sélectionner les professionnels dont elle a la surveillance elle devra pouvoir recourir aux bases de données, telles que le registre du commerce et des sociétés »*[33]. La disposition sous revue est manifestement trop vague et ne respecte dès lors pas le principe de légalité et de prévisibilité qu'exige le droit et la jurisprudence européenne.

b. La coopération entre les autorités luxembourgeoises

En application de l'article 8-2, paragraphe (5) de la loi modifiée du 12 novembre 2004, dans la version modifiée par le projet de loi, l'AED devrait coopérer avec l'Administration des douanes et accises afin d'assurer le contrôle des *« opérateurs en zone franche autorisés à exercer leur activité en vertu d'un agrément de l'Administration des douanes et accises dans l'enceinte de la zone franche douanière communautaire du type contrôle I sise dans la commune de Niederanven section B Senningen au lieu dit Parishaff L-2315 Senningerberg (Hoehenhof) »*. Les deux administrations seraient ainsi autorisées à *« échanger les informations nécessaires à l'accomplissement de leurs missions respectives »*.

Pour le cas où ces échanges comprenaient des données à caractère personnel, la CNPD s'interroge sur la forme ou l'étendue de cette coopération. Les auteurs indiquent dans le commentaire des articles qu'il *« s'avère indispensable de permettre à l'AED d'échanger avec l'ADA toutes les informations indispensables à cet effet comme celles concernant la comptabilité matière des professionnels visés au point 14bis du chapitre 2 de la présente loi »*[34].

Comme noté par les auteurs du projet de loi, les deux administrations coopèrent déjà en vertu de la loi modifiée du 19 décembre 2008 et échangent *« les informations susceptibles de leur permettre l'établissement correct et le recouvrement des droits à l'importation et à l'exportation, des droits d'accises, de la taxe sur les véhicules routiers et de la taxe sur la valeur ajoutée, à l'aide de procédés automatisés ou non »* (article 4 de la loi modifiée du 19 décembre 2008). Le règlement grand-ducal du 3 décembre 2009 concernant la coopération interadministrative de l'Administration de l'Enregistrement et des Domaines et de l'Administration des Douanes et Accises fixe les modalités de cette coopération.

En tenant compte des développements des sections précédentes, la CNPD estime nécessaire d'encadrer la coopération des deux administrations dans le projet de loi, en précisant la forme de cette coopération et les données susceptibles d'être échangées et de prévoir dans un règlement grand-ducal les conditions, critères et modalités de l'échange des données à caractère personnel. Ils pourraient s'inspirer de la prédite loi modifiée du 19 décembre 2008 et de son règlement grand-ducal d'exécution.

[33] Projet de loi n° 7128, doc. parl. n° 7128/00, Commentaire des articles, p. 51.
[34] Projet de loi n° 7128, doc. parl. n° 7128/00, Commentaire des articles, p. 51.

Ces remarques sont également valables pour ce qui est de la coopération générale prévue par l'article 15 du projet loi selon lequel *« les autorités de contrôle et la cellule de renseignement financier coopèrent étroitement. Les autorités de contrôle coopèrent étroitement entre elles.*

Aux fins de l'alinéa 1er, les autorités de contrôle et la cellule de renseignement financier sont autorisées à échanger les informations nécessaires à l'accomplissement de leurs missions respectives dans le cadre de la lutte contre le blanchiment et contre le financement du terrorisme. Les autorités de contrôle et la cellule de renseignement financier utilisent les informations échangées uniquement pour l'accomplissement de ces missions ».

b. Les pouvoirs des autorités

En application de l'article 8-2 de la loi de 2004, tel que modifié par le projet de loi, les autorités de contrôle sont investies de certains pouvoirs, comme, par exemple, le droit d'avoir accès à tout document sous quelque forme que ce soit et d'en recevoir ou prendre copie et le droit de demander des informations à toute personne et, si nécessaire, de convoquer toute personne soumise à leur pouvoir de surveillance respectif conformément à l'article 2-1 et de l'entendre afin d'obtenir des informations[35]. Les autorités de contrôle pourraient encore *« exiger la communication des enregistrement téléphoniques, des communications électroniques ou des enregistrement de données relatives aux trafic détenues par des personnes soumises à leur pouvoir de surveillance respectif conformément à l'article 2-1 »*[36]. Selon le commentaire des articles, cette disposition reprend les pouvoirs que possède la CSSF en vertu de la loi modifiée du 5 avril 1993, en les alignant sur les pouvoirs prévus par l'article 4 de la loi modifiée du 23 décembre 2016 relative aux abus de marché[37].

A cet égard, la Commission nationale tient premièrement à rappeler le considérant 31 du RGPD, selon lequel *« les demandes de communication adressées par les autorités publiques devraient toujours être présentées par écrit, être motivées et revêtir un caractère occasionnel, et elles ne devraient pas porter sur l'intégralité d'un fichier ni conduire à l'interconnexion de fichiers. Le traitement des données à caractère personnel par les autorités publiques en question devrait être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement ».*

Par ailleurs, la CNPD note que le commentaire des articles du projet de loi n° 7022 relative aux abus de marché précisait qu'*« il y a lieu de souligner que le point 6. ne vise que des enregistrements existants. Il ne découle de cette disposition aucune obligation d'enregistrement ou de conservation pour les entités visées au point 6. »*[38]. Une telle indication fait cependant défaut dans le commentaire des articles du présent projet de loi. Nonobstant l'obligation de conservation des pièces justificatifs et enregistrements de transactions et des documents, données et informations relatifs aux mesures de vigilance à l'égard du client, il convient, dans un souci de sécurité juridique, de préciser le projet de loi dans ce sens.

Ces remarques sont également valables pour ce qui est des modifications apportées à la loi modifiée du 10 novembre 2009 relative aux services de paiement[39].

[35] Article 8-2, paragraphe (1), lettre (a) et (b) de la loi modifiée du 12 novembre 2004, tel qu'ajouté résulte du projet de loi.
[36] Voir l'article 8-2, paragraphe (1), lettre (d) de la loi modifiée du 12 novembre 2004, tel qu'ajouté par le projet de loi n° 7128.
[37] Projet de loi n° 7128, doc. parl. n° 7128/00, Commentaire des articles, p. 50.
[38] Projet de loi n° 7022, doc. parl. n° 7022/00, Commentaire des articles, p. 22.
[39] Voir l'article 58-5 de la loi modifiée du 10 novembre 2009 relative aux services de paiement, tel qu'ajouté par le projet de loi n° 7128.

c. La publication des décisions par les autorités de contrôle

Selon l'article 8-6 de la loi modifiée du 12 novembre 2004, tel qu'introduit par projet de loi, les autorités de contrôle, à savoir la CSSF, le CAA et l'AED, auraient l'obligation de publier certaines décisions sur leur site Internet officiel. La CNPD a déjà examiné cette problématique dans le cadre de son avis du 2 décembre 2016 relatif au projet de loi n° 7022 relative aux abus de marché et se réfère dès lors à sa recommandation formulée au point V. dudit avis, notamment en ce qui concerne les données à caractère personnel qui seraient publiées et la durée maximale pendant laquelle les données seraient affichées sur le site Internet de la CSSF.

Ces remarques sont également valables pour ce qui est des modifications apportées à la loi modifiée du 10 novembre 2009 relative aux services de paiement[40].

d. Le signalement des violations aux autorités de contrôle

Il ressort du nouvel article 8-6 de la loi de 2004, tel qu'ajouté par le projet de loi, que les autorités de contrôle devraient mettre en place des *« mécanismes efficaces et fiables pour encourager le signalement des violations potentielles ou avérées des obligations professionnelles en matière de lutte contre le blanchiment et contre le financement du terrorisme par les professionnels soumis à leur pouvoir de surveillance… »*. La CNPD a déjà eu l'occasion de se prononcer sur des mécanismes de *« whistleblowing »* de la CSSF dans le cadre de son avis du 2 décembre 2016 relatif au projet de loi n° 7022 relative aux abus de marché[41]. Elle note que ce projet de loi était accompagné d'une annexe, qui transposait la directive d'exécution (UE) 2015/2392 de la Commission européenne du 17 décembre 2015, prévoyant les modalités et garanties à respecter par la CSSF lors de la mise en place de ces mécanismes.

Afin d'assurer la protection des données traitées et les libertés et droits fondamentaux des personnes concernées, elle estime qu'il y a lieu d'appliquer ces mêmes modalités et garanties aux mécanismes des signalements des violations mis en place par les autorités de contrôle et d'ajouter des dispositions similaires au projet de loi sous avis, sous réserve des recommandations émises par la CNPD à cet égard dans son avis du 2 décembre 2016[42].

Ces remarques sont également valables pour ce qui est des modifications apportées à la loi modifiée du 10 novembre 2009 relative aux services de paiement[43].

Ainsi décidé à Esch-sur-Alzette en date du 18 janvier 2018.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann
Présidente	Membre effectif	Membre effectif

[40] Voir l'article 58-8 de la loi modifiée du 10 novembre 2009 relative aux services de paiement, tel qu'ajouté par le projet de loi n° 7128.
[41] Projet de loi n° 7022, doc. parl. n° 7022/04.
[42] Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7022, doc. parl. n° 7022/04, p. 8.
[43] Voir l'article 58-10 de la loi modifiée du 10 novembre 2009 relative aux services de paiement, tel qu'ajouté par le projet de loi n° 7128.

Avis complémentaire de la Commission nationale pour la protection des données à l'égard du projet de loi n°7113 relatif au Revenu d'inclusion sociale

Délibération n° 59/2018 du 23 janvier 2018

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 ».*

Par courrier du 25 octobre 2017, Madame la Ministre de la Famille et de l'Intégration a fait parvenir à la CNPD une série d'amendements gouvernementaux au projet de loi n° 7113 relatif au Revenu d'inclusion sociale (ci-après « les amendements »).

Pour rappel, la CNPD a rendu, le 22 décembre 2016, un premier avis relatif à l'avant-projet de loi relatif au Revenu d'inclusion sociale[44] dans lequel elle a formulé différentes observations concernant notamment le concept du responsable du traitement, les rôles des différents intervenants dans le processus d'octroi et de gestion du Revenu d'inclusion sociale (ci-après : « le Revis »), les finalités du traitement et les catégories de données traitées, les accès à d'autres fichiers étatiques, ainsi que le transfert de données à l'Inspection générale de la sécurité sociale dans le cadre de sa mission de recueillir des données statistiques. Les auteurs indiquent dans les remarques préliminaires que les amendements apportent, entre autres, une clarification des dispositions relatives à la protection des données à caractère personnel et de leur échange entre les acteurs concernés.

Le commentaire de l'article 25 du projet de loi précise que l'amendement en cause tient compte des remarques formulées dans l'avis de la CNPD du 22 décembre 2016. En effet, la plupart des recommandations émises par la CNPD dans son premier avis concernant ledit article ont été prises en compte par les auteurs des amendements. Les catégories de données des fichiers auxquels le ministre peut accéder sur base de l'article 25, paragraphe (2) du projet de loi, ainsi que les catégories de données contenues dans le fichier du Revis en vertu du paragraphe (1), alinéa 2 dudit article, sont prévues à l'article 9 du projet de règlement grand-ducal, dont les amendements gouvernementaux ont été transmis ensemble avec le projet de loi sous avis.

Par contre, la CNPD émet une réserve concernant la durée de conservation des données contenues dans le fichier du Revis. L'article 25, paragraphe (8) du projet de loi prévoit dans ce contexte que les données sont conservées aussi longtemps que la personne est bénéficiaire du Revis et qu'après, les données seront archivées à des fins statistiques conformément à l'article 12 du projet de loi.

[44] Délibération n° 1029/2016 du 22 décembre 2016 de la Commission nationale pour la protection des données.

Or, il ressort du commentaire des articles que les données seront archivées non pas à des fins statistiques, mais *« afin d'éviter de devoir établir un nouveau rapport social à chaque réouverture de dossier au lieu d'une actualisation, l'archivage, contrairement à la suppression des données, permet la reprise des données à la réactivation du dossier. »* Est-ce que la finalité poursuivie par l'archivage est donc l'établissement de statistiques ou plutôt la possibilité d'une réouverture plus facile d'un dossier d'un ancien demandeur ou bénéficiaire du Revis ?

La CNPD peut comprendre l'utilité pratique d'un archivage temporaire des données permettant de réactiver un dossier d'un ancien demandeur ou bénéficiaire du Revis, par rapport à leur suppression immédiate après la clôture d'un dossier. Néanmoins, selon l'article 4, paragraphe (1), lettre d) de la loi modifiée du 2 août 2002, les données ne doivent pas être conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Ce principe est incompatible avec une durée de conservation indéterminée des données. En effet, la CNPD est d'avis que la réalisation des finalités prévues à l'article 25, paragraphe (1), alinéa 3 du projet de loi sous examen ne justifie pas un archivage des données personnelles à durée indéterminée.

Il est important dans ce contexte de prendre en compte, à l'instar de la position de la Commission Nationale de l'Informatique et des Libertés (CNIL) française, la différence entre les archives intermédiaires, une étape intermédiaire avant la suppression des données, et les archives définitives qui rassemblent les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction[45]. Est-ce que l'archivage prévu par les auteurs des amendements constitue un archivage intermédiaire, permettant pendant une durée déterminée la réouverture d'un dossier d'un ancien demandeur ou bénéficiaire du Revis, ou plutôt un archivage définitif ?

Dans le cas d'un archivage définitif, la CNPD estime qu'uniquement des données anonymisées peuvent être archivées de manière définitive à des fins statistiques. En sus, lors d'un archivage intermédiaire des données, il est important que seulement les personnes ayant un intérêt à les connaitre en raison de leurs fonctions en ont accès. Dans ce dernier cas, la question se pose si les données seront conservées sous forme pseudonymisée ou de manière nominative permettant directement d'identifier les personnes concernées ?

Ainsi, la CNPD suggère aux auteurs des amendements d'énoncer dans le corps du texte du projet de loi d'un côté pour quelle durée précise les données des demandeurs ou bénéficiaires du Revis seront conservées dans la base de données active et opérationnelle du fichier du Revis, et d'autre côté pendant combien de temps elles seront conservées dans les archives intermédiaires et si une anonymisation complète des données à des fins d'archivage définitif sera prévue après un certain délai. Notons encore que la durée de conservation des données à titre d'archivage intermédiaire devra être limitée à une ou deux années, alors qu'une durée plus longue ne serait pas compatible avec le principe que les données doivent être exactes et à jour.

[45] Voir sur le site internet de la CNIL « Limiter la conservation des données », disponible sous : https://www.cnil.fr/fr/limiter-la-conservation-des-donnees.

Par ailleurs, la CNPD regrette que les observations formulées à l'occasion de son premier avis concernant les articles 26 et 49 (l'actuel article 51) n'ont pas été intégrées dans le projet de loi. A ce titre, elle avait formulé dans son avis du 22 décembre 2016 les commentaires suivants :

« Selon l'article 26, l'Office communique sur autorisation du Ministre de la Famille et de l'Intégration des données pseudonymisées à l'Inspection générale de la sécurité sociale qui peut en disposer dans le cadre de sa mission de recueillir des données statistiques nécessaires sur le plan national et international « suivant un plan statistique et comptable uniforme pour toutes les institutions sociales » (article 423, point (4) du Code de la sécurité sociale).

Dans ce contexte, la CNPD attire l'attention sur la différence entre données pseudonymisées et anonymisées. Selon le groupe de travail «article 29» sur la protection des données « l'anonymisation est le résultat du traitement des données personnelles afin d'empêcher, de façon irréversible, toute identification » alors que « la pseudonymisation n'est pas une méthode d'anonymisation. Elle réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée et constitue par conséquent une mesure de sécurité utile. »[46]

Contrairement aux données anonymes, les données simplement pseudonymisées tombent toujours sous le champ d'application de la loi modifiée du 2 août 2002.

Dès lors, la CNPD se pose la question si l'établissement de statistiques nationales et internationales, justifie la communication des données pseudonymisées? Une communication de données anonymes ne serait-elle pas suffisante ?

Ce texte n'est pas assez précis pour pouvoir déterminer quelles données devraient, le cas échéant, être communiquées, sous forme pseudonymisée, à des fins statistiques à l'IGSS. Dans sa rédaction actuelle, l'ONIS, devrait, sur demande de l'IGSS, communiquer l'intégralité de ses données (sous forme pseudonymisée) à l'IGSS. Se pose dès lors la question de la nécessité et de la proportionnalité des données communiquées.

Les mêmes observations ci-dessus sont également valables pour ce qui est de l'article 49 qui introduit aussi une communication sur autorisation des données pseudonymisées contenues dans les fichiers des offices sociaux à l'IGSS. »

Finalement, la CNPD constate que l'amendement 20 prévoit d'ajouter un article 17ter à la loi modifiée du 30 juillet 1960 concernant la création d'un fonds national de solidarité, permettant audit fonds d'accéder dans le cadre de l'exercice de ses missions, par voie d'interconnexions, à divers fichiers étatiques. Le paragraphe (3) de l'article en cause ajoute que *« les informations accédées, doivent être limitées aux données nécessaires à l'instruction du droit à l'une des prestations du Fonds, à son paiement, son contrôle et à la révision des conditions d'accès. »*

[46] Groupe de travail «article 29» sur la protection des données, avis 05/2014 sur les Techniques d'anonymisation adopté le 10 avril 2014, p.

La CNPD 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. »*[47]

Le Conseil d'État 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 (…). »[48]

Sur base des considérations ci-dessus, la CNPD estime que l'article 17*ter* de la loi modifiée du 30 juillet 1960 concernant la création d'un fonds national de solidarité devrait énumérer pour chaque fichier étatique visé, les données à caractère personnel auxquelles le Fonds national de solidarité peut accéder. Cet accès devrait être limité aux données qui sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement (article 4, paragraphe (1) lettre b) de la loi modifiée du 2 août 2002).

La CNPD estime ainsi qu'en l'état actuel, l'article 17*ter* de ladite loi modifiée du 30 juillet 1960 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.

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

Ainsi décidé à Esch-sur-Alzette en date du 23 janvier 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif

[47] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015
[48] Voir par exemple : Conseil d'État, 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'État pour études supérieures.

Avis de la Commission nationale pour la protection des données à l'égard de l'avant-projet de règlement grand-ducal relatif à l'organisation et les méthodes de travail du service national de coordination des dons d'organes

Délibération n° 79/2018 du 31 janvier 2018

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

Faisant suite à la demande lui adressée par Madame la Ministre de la Santé en date du 20 septembre 2017, la CNPD entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de règlement grand-ducal relatif à l'organisation et les méthodes de travail du service national de coordination des dons d'organes.

Cet avant-projet de règlement grand-ducal a pour objet de définir l'organisation et les méthodes de travail du service national de coordination du prélèvement et de la transplantation d'organes (ci-après, le « service national de coordination »). Ce service national de coordination a notamment pour mission de consigner sous forme électronique les données visées à l'annexe I du règlement grand-ducal du 27 août 2013 concernant la caractérisation, le transport et l'échange d'organes destinés à la transplantation (article 2 paragraphe (2), 2ème tiret, 2ème alinéa). De plus, il établit et tient à jour une liste des coordinateurs impliqués dans la transplantation et le prélèvement d'organes, et une liste des malades en attente d'une greffe d'organes (article 3).

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par les articles 2, 3 et 7 de l'avant-projet de règlement grand-ducal sous examen.

1. Remarque préliminaire

A titre préliminaire, la CNPD souhaite relever que les articles précités de l'avant-projet de règlement grand-ducal visent à créer un nouveau fichier de données à caractère personnel au sens de l'article 2 lettre (h) de la loi du 2 août 2002 et de l'article 4 point (6) du Règlement Général sur la Protection des Données (UE) 2016/679 du 27 avril 2016, qui sera applicable à partir du 25 mai 2018 dans tous les États membres de l'Union européenne (ci-après : « le RGPD »).

Elle 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 »*[49]. 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 »*[50]. *« Le degré de précision requis de la « loi » à cet égard dépendra du sujet en question. »*[51]

Dans le même sens, l'article 6, paragraphe (3) du RGPD prévoit cette 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, la limitation des finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

La Commission nationale considère que la loi modifiée du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine, en particulier dans ses articles 15 et suivants, constitue une base légale suffisamment accessible et prévisible, à condition que l'avant-projet de règlement grand-ducal sous examen précise à suffisance

[49] 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.

[50] 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.

[51] 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.

le responsable du traitement, les finalités du traitement, les catégories de données traitées, l'origine des données, les personnes ayant accès aux données et la durée de conservation des données. Pour chacun de ces éléments, la CNPD entend détailler ci-après ses observations.

2. Le responsable du traitement

L'article 2 paragraphe (2), 2ème tiret, 3ème alinéa de l'avant-projet de règlement grand-ducal sous examen prévoit que *« le service national de coordination est responsable du traitement des données médicales qui sont consigné[es] sous forme électronique suite à la caractérisation des donneurs d'organes et des organes, au sens de la loi modifiée du 2 août [2002] relative à la protection des personnes à l'égard du traitement des données à caractère personnel ».*

L'article 7 paragraphe (2), 2ème alinéa du même avant-projet indique quant à lui que *« les établissements hospitaliers sont responsables du traitement et du transfert des données personnelles contenues dans le dossier individuel aux acteurs impliqués dans le prélèvement et la [transplantation] d'organes prévu[s] aux paragraphes précédents, 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 ».*

Enfin, l'article 3, 2ème tiret, alinéas 3 et 4, précise que *« les établissements hospitaliers sont responsable[s] du transfert des données administratives du dossier médical au sens de loi modifiée du 2 août [2002] (…) », tandis que « le service national de coordination est responsable du traitement des données administratives du dossier médical au sens de loi modifiée du 2 août [2002] (…) ».*

La Commission nationale ne comprend pas cette distinction opérée par les auteurs de l'avant-projet de règlement grand-ducal entre données médicales d'une part, et données administratives (du dossier médical) d'autre part. Les auteurs de l'avant-projet de loi n'expliquent d'ailleurs pas ce qu'il faut entendre par données « administratives ». L'ensemble des différentes données visées constituent en tout état de cause des données à caractère personnel. De plus, les données médicales, ou données relatives à la santé au sens de l'article 6 de la loi du 2 août 2002 et de l'article 9 du RGPD, sont évidemment liées à une personne identifiée. Il apparaît donc artificiel de séparer les données médicales des données dites « administratives ».

Par ailleurs, la distinction entre « responsable du traitement » et « responsable du transfert » n'apparaît pas opportune. En effet, alors que la notion de responsable du traitement renvoie à la définition de l'article 2 lettre (n) de la loi du 2 août 2002, et de l'article 4 numéro (7) du RGPD, celle de « responsable du transfert » ne correspond pas à une terminologie utilisée dans ces législations. En outre, tout transfert constituant une opération de traitement, la notion de « responsable du transfert » apparaît superflue.

Sur base de ces considérations, la Commission nationale suggère aux auteurs de l'avant-projet de règlement grand-ducal de remplacer les passages précités par une seule disposition, selon laquelle le service national de coordination est le responsable du traitement relatif aux données appelées à figurer dans le fichier de données à caractère personnel concernant les dons d'organe.

Enfin, la CNPD se demande si les établissements hospitaliers doivent être considérés comme les fournisseurs des données appelées à figurer dans le fichier de données à caractère personnel concernant les dons d'organe, dans la mesure où le dossier patient dont l'établissement hospitalier est le responsable du traitement renseigne de toute évidence déjà des informations relatives à l'état de santé du patient respectivement la nécessité d'une greffe d'organe ? Ou s'ils doivent être considérés comme sous-traitants, traitant certaines données pour le compte du service national de coordination ? En tout état de cause, il conviendrait de clarifier leur rôle dans l'avant-projet de règlement grand-ducal sous objet.

3. Les finalités du traitement

L'article 2 de l'avant-projet de règlement grand-ducal prévoit le rôle et les missions du service national de coordination. Ce dernier a notamment pour mission de consigner sous forme électronique les données visées à l'annexe I du règlement grand-ducal du 27 août 2013 concernant la caractérisation, le transport et l'échange d'organes destinés à la transplantation (article 2 paragraphe (2), 2ème tiret, 2ème alinéa). L'article 3 y ajoute l'établissement et la mise à jour d'une liste des coordinateurs impliqués dans la transplantation et le prélèvement d'organes, et d'une liste des malades en attente d'une greffe d'organes.

La Commission nationale comprend qu'il s'agit là des finalités des traitements de données qui seront mis en œuvre par le service national de coordination.

4. Les catégories de données traitées

L'article 2, paragraphe (2), 2ème tiret se réfère à l'article premier du règlement grand-ducal du 27 août 2013 précité, ainsi qu'à son annexe I. Ladite annexe I liste de façon exhaustive l'ensemble des données à caractère personnel traitées pour la caractérisation des organes et des donneurs.

Elle se subdivise en une partie A contenant les données minimales, c'est-à-dire les informations qui doivent être collectées pour chaque don, et une partie B qui contient les données complémentaires, c'est-à-dire les informations qui doivent être collectées en plus des données minimales selon la décision de l'équipe médicale, en tenant compte de la disponibilité de ces informations et des circonstances particulières de l'espèce.

Il ressort de l'article 3 qu'une liste des coordinateurs impliqués dans la transplantation et le prélèvement d'organes,

et une liste des malades en attente d'une greffe d'organes sont également traitées par le service national de coordination. Cet article n'indique cependant pas si cette liste contient uniquement les données de contact des coordinateurs et des malades en attente de greffe, ou d'autres données à caractère personnel y associées. La Commission nationale estime indispensable d'indiquer précisément quelles sont les catégories de données traitées dans ce cadre.

L'article 3 se réfère également à des *« données administratives du dossier médical »*. Il ressort du commentaire des articles que ces données *« se rapportent aux données recueillies lors de l'examen clinique, à savoir les données obtenues lors de l'anamnèse (l'interrogatoire du patient sur son état de santé) ainsi que les données médicales (plus précisément les données paracliniques) obtenues lors d'examens complémentaires »*. Comme plus amplement expliqué dans la section 1 du présent avis, la Commission nationale ne comprend pas cette distinction entre « données administratives » et « données médicales », et propose dès lors de se référer dans l'article en question à l'ensemble des données qui sont traitées par le service national de coordination.

5. <u>L'origine des données</u>

Il ressort de l'article 1er du règlement grand-ducal du 27 août 2013 précité que les données visées à l'article 2, paragraphe (2), 2ème tiret de l'avant-projet de règlement grand-ducal sous objet *« sont collectées par les établissements de prélèvement pour chaque don d'organes »*.

L'article 3, 2ème tiret, alinéa 2, de l'avant-projet de règlement grand-ducal sous examen prévoit quant à lui que les données administratives du dossier médical proviennent des établissements hospitaliers du pays. Comme indiqué dans la section 1 du présent avis, la Commission nationale ne comprend cependant pas si cela signifie que les établissements hospitaliers doivent être considérés comme fournisseurs de certaines données, ou comme sous-traitants, traitant dans ce cas ces données pour le compte du service national de coordination ?

Par ailleurs, la CNPD se réfère aux sections 1 et 4 du présent avis, où elle exprime ses interrogations quant à la distinction réalisée entre « données administratives » et « données médicales ». Par conséquent, elle estime indispensable de préciser l'origine de toutes les données traitées par le service national de coordination, et non des seules *« données administratives du dossier médical »*.

6. <u>Les personnes ayant accès aux données</u>

Ni l'article 2, ni l'article 3 de l'avant-projet de règlement grand-ducal sous examen ne précisent quelles sont les personnes qui auront accès au fichier de données à caractère personnel concernant les dons d'organe, outre le service national de coordination lui-même.

Dans l'hypothèse où certaines données pourraient être transmises à des tiers, la Commission nationale estime indispensable de le préciser dans l'avant-projet de règlement grand-ducal sous objet.

7. La durée de conservation des données

L'article 3, deuxième tiret, alinéa 5 de l'avant-projet de règlement grand-ducal sous examen prévoit que les données administratives du dossier médical seront conservées *« pour une durée minimale de 30 ans et pour une durée maximale de 50 ans »*. En l'absence de justification de ces durées de conservation dans le commentaire des articles, la Commission nationale n'est pas en mesure d'apprécier le caractère proportionné des durées de conservation des données administratives du dossier médical.

Par ailleurs, elle ne comprend pas la raison d'être d'une telle disparité entre les durées de conservation. A moins que les auteurs de l'avant-projet de loi sous objet justifient pourquoi dans certains cas, les données doivent être conservées 30 ans et dans d'autres 40 ou 50 ans, la CNPD privilégie l'option consistant à prévoir une seule durée de conservation pour l'ensemble des données traitées. Sans explication supplémentaire, une telle disparité entre les durées de conservation n'aurait en effet pas de sens aux yeux de la Commission nationale.

Par contre, l'avant-projet de règlement grand-ducal ne prévoit pas de durée de conservation pour les autres données visées à l'article 3, à savoir la liste des coordinateurs impliqués dans la transplantation et le prélèvement d'organes, et la liste des malades en attente d'une greffe d'organes.

De même, l'article 2 n'indique pas pour combien de temps le service national de coordination doit consigner sous forme électronique les données dont il est fait référence à l'annexe I du règlement grand-ducal précité du 27 août 2013.

La Commission nationale estime nécessaire de prévoir l'ensemble des durées de conservation relatives aux catégories de données précitées. Les données ne pourront en tout état de cause être « conservées sous une forme permettant l'identification des personnes concernées [que] pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées », conformément à l'article 4, paragraphe (1), lettre (d) de la loi du 2 août 2002.

Ainsi décidé à Esch-sur-Alzette en date du 31 janvier 2018.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann
Présidente	Membre effectif	Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal relatif à la radioprotection

Délibération n° 138/2018 du 23 février 2018

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

Par courrier en date du 20 septembre 2017, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal relatif à la radioprotection (ci-après le « projet de règlement grand-ducal »).

Le projet de règlement grand-ducal vise à transposer en droit national la directive 2013/59/Euratom du 5 décembre 2013 dont l'échéance a été fixée à la date du 6 février 2018 et il exécutera la future loi 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 sur relatif à la radioprotection ») qui a fait l'objet d'un avis de la Commission nationale au date du 14 juillet 2017 (délibération n° 596/2017).

Les objectifs principaux du projet de règlement grand-ducal sont d'établir *« un cadre juridique national en matière de la protection sanitaire des personnes contre les dangers résultants de l'exposition aux rayonnements ionisants et à la sécurité des sources de rayonnements ionisants contre les actes de malveillance »*[52].

Pour sa part, la Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de règlement grand-ducal sous examen traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel.

I) Le service de dosimétrie :

Les données concernées :

La Commission nationale comprend que le rôle du service de dosimétrie peut, inter alia, être assuré par un service

[52] *cf.* Exposé des motifs, dernière phrase.

externe autorisé par le ministre selon les critères précisés à l'article 11 du projet de règlement grand-ducal. La CNPD n'est pas en mesure de déterminer si le principe de minimisation des données a été respecté alors que les articles 9 à 11 du projet de règlement grand-ducal ne précisent pas les données exactes communiquées à un tel service de dosimétrie.

En outre, l'article 39 paragraphe (3) chiffre (5°) du projet de règlement grand-ducal indique que les services de dosimétrie autorisés bénéficient aussi d'un accès au registre de dosimétrie centrale *« en ce qui concerne les données visées par le présent article, qu'ils fournissent »*. Pour ce qui est du service de dosimétrie, il ne ressort pas de cet article quelles données exactes sont communiquées au registre de dosimétrie central. De ce fait, la Commission nationale ne peut pas se prononcer sur la légitimité des traitements des données effectuées par le service de dosimétrie.

II) Le registre de dosimétrie central :

L'article 38 paragraphe (2) du projet de règlement grand-ducal indique les données relatives à l'identité des travailleurs exposés et mentionne qu'un numéro d'identification unique sera inclus dans le registre de dosimétrie central. S'il s'agit du numéro d'identité national, la Commission nationale recommande que le texte de cet article fasse référence à 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.

La CNPD accueille favorablement que l'accès au registre de dosimétrie central de chaque acteur soit limité aux données telles que précisées à l'article 39 paragraphe (3) du projet de règlement grand-ducal. Toutefois, la Commission nationale renvoie à son commentaire sous le point I) du présent avis en ce qui concerne les services de dosimétrie.

En outre, la Commission nationale note que toutes les personnes soumises à la surveillance dosimétrique auront accès aux données les concernant et, par conséquent, aussi les travailleurs extérieurs (qui n'ont pas de relation directe avec le chef d'établissement).

La CNPD remarque à toutes fins utiles qu'à l'article 39 paragraphe (3) chiffres (2°) et (3°) et (4°) les auteurs du projet de règlement grand-ducal ont certainement voulu faire référence à l'article 38 au lieu de l'article 37. Il en va de même pour la mention de l'article 37 à l'article 40 paragraphe (2) du projet de règlement grand-ducal. Par ailleurs, l'article 38 paragraphe (1) fait référence à un paragraphe (6) qui n'existe pas dans cet article.

III) Le carnet radiologique :

La Commission nationale s'interroge pourquoi le projet de règlement grand-ducal ne contient pas de dispositions concernant le carnet radiologique électronique, alors que, selon l'exposé des motifs, le projet de règlement grand-

ducal est censé exécuter aussi la troisième partie du projet de loi relatif à la radioprotection qui concerne la création d'un carnet radiologique électronique.

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

Ainsi décidé à Esch-sur-Alzette en date du 23 février 2018.

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 règlement grand-ducal portant fixation des indemnités revenant au Président, aux membres et aux membres suppléants de la Commission nationale pour la protection des données et abrogeant le règlement grand-ducal du 7 juillet 2003

Délibération n° 139/2018 du 1er mars 2018

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

Par courrier en date du 11 janvier 2018, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal portant fixation des indemnités revenant au Président, aux membres et aux membres suppléants de la Commission nationale pour la protection des données (ci-après le « projet de règlement grand-ducal »).

L'adoption au niveau européen du paquet législatif sur la protection des données, englobant le règlement (UE) 2016/679 et la directive (UE) 2016/680, aura comme conséquence que la législation nationale devra être abrogée. En effet, le règlement (UE) 2016/679 sera d'application directe à partir du 25 mai 2018. Or, le règlement (UE) 2016/679 devra être accompagné par une loi de mise en œuvre afin de trouver une bonne application au niveau national. Ce projet de *loi 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'État et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personne* (ci-après « le projet de loi ») comportera essentiellement les dispositions nécessaires quant à l'organisation et la composition de la Commission nationale pour la protection des données.

Le présent projet de règlement grand-ducal s'inscrit dès lors dans la mise en œuvre des articles 23 et 27 du projet de loi qui prévoient que des indemnités reviennent au Président, aux membres autre que le Président et aux membres suppléants de la Commission nationale pour la protection des données.

En vertu de l'article 23 deuxième alinéa du projet de loi 7184, l'indemnité tient compte de l'engagement requis par les fonctions.

Le projet de règlement grand-ducal sous avis est une copie exacte du règlement grand-ducal du 7 juillet 2003 portant fixation des indemnités revenant au président, aux membres effectifs et aux membres suppléants de la Commission nationale pour la protection des données qu'il s'agit à présent d'abroger.

En effet, le règlement grand-ducal de 2003 avait été pris en exécution des articles 34 paragraphe (2) alinéas 10 et 12 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, qui contiennent des dispositions similaires à celles des articles 23 et 27 de la future loi organique de la CNPD.

La Commission nationale n'entend pas se prononcer sur les indemnités revenant au président et membres (effectifs) de la Commission nationale. Elle tient seulement à remarquer que par l'effet de l'indexation automatique et les augmentations successives de la valeur du point, l'indemnisation prévue en 2003 n'a pas perdu en valeur avec le temps.

Il en est autrement pour ce qui est de l'indemnisation des membres suppléants, exprimée non pas en points, mais en euros, pour lesquels il y a lieu de se poser la question si le montant de 60,- € prévu en 2003 par vacation horaire, tient encore compte de l'engagement requis par cette fonction.

Pour ce qui est de la forme, la Commission nationale rejoint le commentaire formulé par la Chambre des fonctionnaires et employés publics en ce qu'à l'article 1 paragraphe (1) du projet de règlement grand-ducal le mot « cents » est à supprimer. Il y a également lieu d'enlever les signes «.- » derrière 150 et 120.

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

Ainsi décidé à Esch-sur-Alzette en date du 1er mars 2018.

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 règlement grand-ducal portant fixation du siège de la Commission nationale pour la protection des données et abrogeant le règlement grand-ducal du 7 juillet 2003 portant transfert du siège de la Commission nationale pour la protection des données

Délibération n° 140/2018 du 1er mars 2018

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

Par courrier en date du 11 janvier 2018, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal portant fixation du siège de la Commission nationale pour la protection des données et abrogeant le règlement grand-ducal du 7 juillet 2003 portant transfert du siège de la Commission nationale pour la protection des données (ci-après le « projet de règlement grand-ducal »).

L'adoption au niveau européen du paquet législatif sur la protection des données, englobant le règlement (UE) 2016/679 et la directive (UE) 2016/680, aura comme conséquence que la législation nationale devra être abrogée. En effet, le règlement (UE) 2016/679 sera d'application directe à partir du 25 mai 2018. Or, le règlement (UE) 2016/679 devra être accompagné par une loi de mise en œuvre afin de trouver une bonne application au niveau national. *Ce projet de loi 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'État 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 ») comportera essentiellement les dispositions nécessaires quant à l'organisation et la composition de la Commission nationale pour la protection des données.

Le présent projet de règlement grand-ducal s'inscrit dans la mise en œuvre de l'article 2 du projet de loi en ce qu'il convient de fixer le siège de la Commission nationale pour la protection des données.

Aux termes dudit article 2, le siège de la Commission nationale pour la protection des données sera fixé par règlement grand-ducal. L'article 1 du présent projet de règlement grand-ducal fixe le siège de la Commission nationale à Esch-sur-Alzette.

La formulation reprend les termes du règlement grand-ducal du 7 juillet 2003 portant transfert du siège de la Commission nationale pour la protection des données, règlement grand-ducal que les auteurs du projet sous avis projettent par ailleurs d'abroger.

La Commission nationale tient à remarquer qu'elle est d'ores et déjà installée à Esch-sur-Alzette au Bâtiment administratif de l'État sis 1, Avenue du Rock'n'Roll, ainsi qu'à l'ancien « Container du Fonds Belval », sis 6, avenue des Hauts Fourneaux. S'il est vrai qu'elle est à la recherche d'une solution qui permette le regroupement et l'expansion des effectifs de la Commission nationale, cette solution pourrait très bien se trouver à Esch-sur-Alzette.

Au vu de ce qui précède, le maintien du siège à Esch-sur-Alzette convient.

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

Ainsi décidé à Esch-sur-Alzette en date du 1er mars 2018.

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 à l'égard du projet de loi relative à des mesures macroprudentielles portant sur les crédits immobiliers résidentiels et portant modification de la loi modifiée du 5 avril 1993 relative au secteur financier, et de la loi du 1er avril 2015 portant création d'un comité du risque systémique et modifiant la loi modifiée du 23 décembre 1998 relative au statut monétaire et à la Banque centrale du Luxembourg

Délibération n° 220/2018 du 29 mars 2018

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

Faisant suite à la demande lui adressée par Monsieur le Ministre des Finances en date du 12 décembre 2017, la CNPD entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi relative à des mesures macroprudentielles portant sur les crédits immobiliers résidentiels et portant modification de la loi modifiée du 5 avril 1993 relative au secteur financier, et de la loi du 1er avril 2015 portant création d'un comité du risque systémique et modifiant la loi modifiée du 23 décembre 1998 relative au statut monétaire et à la Banque centrale du Luxembourg.

Ce projet de loi a pour objectif de compléter le dispositif législatif en matière d'outils macroprudentiels à disposition des autorités luxembourgeoises par l'introduction de mesures macroprudentielles pouvant être utilisées spécifiquement en cas de menace pour la stabilité financière du système financier national émanant d'évolutions dans le secteur immobilier au Luxembourg.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'article 2 du projet de loi sous examen.

Cet article introduit un droit d'accès de la Banque centrale du Luxembourg (ci-après : « la BCL ») *« à des <u>informations agrégées</u> disponibles auprès d'administrations étatiques, d'établissements publics autres que ceux placés sous la surveillance des communes et d'autres autorités étatiques compétentes pour autant que ces informations soient nécessaires à ses activités de recherche et d'analyses en relation avec la mission du comité du risque systémique ».*

Les auteurs du projet de loi sous objet justifient ce droit d'accès dans l'exposé des motifs par la nécessité pour la BCL d'effectuer des analyses et études *« afin d'identifier au plus tôt les risques systémiques qui peuvent apparaître dans le système financier ».* Or, *« la mise en place d'un tel cadre ne va pas sans accès à un éventail de données ».*

La Commission nationale constate que ce droit d'accès élargi de la BCL se limite à des *« informations agrégées »*. Sans plus de précisions sur ce qu'il faut entendre par *« informations agrégées »*, elle se demande si ces termes correspondent à des données **anonymisées** ou à des données **pseudonymisées** ?

La distinction entre données anonymes ou anonymisées, d'une part, et données pseudonymisées, d'autre part, est importante. En effet, cette distinction détermine l'applicabilité de la loi du 2 août 2002, et, à compter du 25 mai 2018, du règlement général sur la protection des données 2016/679 (UE) (ci-après : « le RGPD »). La loi comme le RGPD s'appliquent aux traitements de données à caractère personnel, c'est-à-dire à toute information se rapportant une personne physique identifiée ou identifiable (dénommée « personne concernée ») (article 2 (e) de la loi et article 4 (1) du RGPD).

Il en ressort qu'une donnée pseudonymisée tombe sous la définition de la donnée à caractère personnel dès lors que la personne concernée peut être identifiée ou identifiable. Lorsque l'on parle de données pseudonymisées, il peut en effet être possible de retrouver l'identité d'une personne. Il en va ainsi, par exemple, s'il existe une liste de concordance entre les données pseudonymisées et la personne concernée. Il est important de constater que, même si le responsable du traitement (dans ce cas la BCL) ne met pas effectivement en œuvre de moyens pour identifier la personne concernée, ou ne possède pas lui-même de liste de concordance, la personne concernée est susceptible d'être réidentifiée par tous moyens, par exemple par l'analyse et le rapprochement des différentes variables utilisées et collectées dans un éventail de données. Dès lors, la loi comme le RGPD s'applique aux données pseudonymisées, puisqu'il s'agit de données à caractère personnel au sens de l'article 2 (e) de la loi et de l'article 4 point (1) du RGPD. Le fait de pseudonymiser ou de coder les données peut toutefois constituer une garantie appropriée destinée à renforcer la confidentialité et la sécurité des traitements au sens des articles 22 et 23 de la loi ou de l'article 32[53] du RGPD.

Une donnée anonyme ou anonymisée est au contraire exclue du champ d'application de la loi ou du RGPD. Pour être réputée anonyme ou rendue anonyme, il faut qu'il s'agisse d'une donnée pour laquelle il n'existe aucun moyen technique, soit dans le chef du responsable du traitement (c'est-à-dire de la BCL), soit même dans le chef d'un tiers (par exemple l'administration étatique ou l'établissement public duquel proviennent les données), permettant de rattacher cette donnée à un individu. Il appartient au responsable du traitement d'apporter la preuve que les données qu'il traite sont à qualifier de données anonymes. On parle alors d'anonymisation irréversible, faite, par exemple, par des techniques de hachage.

En effet, aux termes du considérant 26 du RGPD[54], *« il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une*

[53] Voir en particulier l'article 32 paragraphe (1) lettre (a) du RGPD.
[54] Voir également le considérant 26 de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, qui a été transposée par la loi du 2 août 2002 en droit national.

personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche ».

Dès lors, la CNPD suggère de préciser, au regard des observations apportées ci-avant, si le projet de loi sous objet entend permettre à la BCL d'accéder à des données anonymisées ou pseudonymisées.

S'il s'agit de données anonymisées, la Commission nationale propose de remplacer les termes *« informations agrégées »* par *« données agrégées et anonymisées »*, afin d'ôter toute ambiguïté possible sur la nature des données qui pourraient faire l'objet d'un droit d'accès par la BCL. Dans ce cas, la loi, ou à compter du 25 mai 2018, le RGPD, n'aurait pas vocation à s'appliquer à la collecte de telles données.

Toutefois, au cas où les *« informations agrégées »* devraient être qualifiées de données pseudonymisées, la loi de 2002, respectivement le RGPD à partir du 25 mai 2018, s'appliquera avec toutes les conséquences qui en découlent. Si tel était le cas, la disposition sous examen serait manifestement trop vague et ne respecterait dès lors pas le principe de légalité et de prévisibilité qu'exige le droit et la jurisprudence européenne. En effet, comme l'explique le considérant 41 du RGPD, une base juridique ou une mesure législative qui sert de base à un traitement 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 et de la Cour européenne des droits de l'homme »*. Afin de satisfaire à ces critères, les auteurs du projet de loi sous objet pourraient dans cette hypothèse se référer à d'autres projets de loi récents au sujet desquels la Commission nationale pour la protection des données a publié un avis[55].

Ainsi décidé à Esch-sur-Alzette en date du 29 mars 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif

[55] Voir par exemple l'avis de la CNPD du 7 décembre 2017 relatif au projet de loi n° 7182 portant modification de la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'État et de dispositions diverses (délibération 973/2017), ou encore l'avis de la CNPD du 18 janvier 2018 relatif au projet de loi n° 7128 (délibération 51/2018).

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé

Délibération n° 242/2018 du 5 avril 2018

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

Par courrier en date du 28 septembre 2017, Monsieur le Ministre de la Sécurité Sociale a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé (ci-après « le projet de règlement grand-ducal » ou « le projet »).

Ce projet pose le cadre règlementaire applicable au dossier de soins partagé (ci-après « le DSP »). Il est pris en application de l'article 60quater du Code de la sécurité sociale, introduit par la loi du 17 décembre 2010 portant réforme du système de soins de santé[56].

Le projet de règlement grand-ducal détaille les modalités et conditions de mise en place du DSP. Il fixe ainsi les grands principes applicables à la création du DSP (article 2), à son activation et son accès par le titulaire dudit dossier (article 3), à sa fermeture et suppression (article 4), à l'accès au DSP par les professionnels de santé (article 5), aux droits d'accès, d'écriture et d'opposition du titulaire (article 6), aux titulaires mineurs non émancipés et titulaires majeurs protégés par la loi (article 7), aux droits d'accès et d'écriture des professionnels de santé (article 8), à la traçabilité des accès et des actions (article 9), au délai de versement des données au DSP (article 10), à la sécurité de la plateforme électronique nationale (article 11), aux modalités techniques de versements des données au DSP et interopérabilité (article 12) et à la coopération et échanges transfrontaliers (article 13).

Pour rappel, la Commission nationale a rendu, le 24 novembre 2010[57], un avis relatif au projet de loi portant réforme du système de soins de santé dans lequel elle a formulé ses observations concernant la mise en œuvre du DSP.

La CNPD relève 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

[56] Loi du 17 décembre 2010 portant réforme du système de soins de santé (Mémorial A-2010-242 du 27 décembre 2010, p. 4041, doc. parl. 6196).
[57] Délibération n° 345/2010 du 24 novembre 2010 portant avis de la CNPD sur le projet de loi 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, doc. parl. 6196/04.

directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD ») sera applicable dans tous les États membres de l'Union européenne à partir du 25 mai 2018.

Ainsi, elle considère qu'il n'y a plus aucun intérêt à analyser le projet de règlement grand-ducal à la lumière de la loi modifiée du 2 août 2002 qui est la législation actuellement en vigueur, mais uniquement sur base des dispositions du RGPD.

La Commission nationale entend limiter ses observations aux dispositions du projet de règlement grand-ducal ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel. Elle se propose de suivre l'ordre de rédaction du projet de règlement grand-ducal pour exprimer ses recommandations.

X. Remarques préliminaires

a. Base de légitimité de la création du DSP

L'article 60*quater* du Code de la sécurité sociale, ainsi que les dispositions du règlement grand-ducal sous examen prévoient qu'un DSP sera activé d'office pour tout patient dès son affiliation à l'assurance maladie luxembourgeoise et qu'il n'a pas signalé son opposition (système de l' « opt-out »), à l'inverse de la solution du législateur français qui a opté de baser la création d'un dossier électronique pour les bénéficiaires de l'assurance maladie sur leur consentement préalable[58] (système de l' « opt-in »).

Il n'appartient pas à la CNPD de commenter le choix politique fait par le législateur en 2010, en optant pour un système d'opt-out. Il convient cependant d'analyser si un système d'opt-out introduit à l'époque sous la directive 95/46[59] et la loi modifiée du 2 août 2002 est toujours compatible avec les dispositions du RGPD qui sera applicable à partir du 25 mai 2018.

Contrairement à la position de la Chambre des salariés exprimée dans son avis du 14 novembre 2017, ainsi que celle de l'Association des Médecins et Médecins-Dentistes (AMMD), de la COPAS et du Syndicat des Pharmaciens Luxembourgeois, exposée dans une lettre adressée au Président de la Commission européenne, Monsieur Jean-Claude Juncker, en date du 4 janvier 2018, la CNPD ne voit *a priori* pas d'incompatibilité de principe avec le RGPD, et ce pour les raisons qui suivent.

Tout d'abord, l'article 6 paragraphe (3) du RGPD, 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 les finalités des traitements de données

[58] Articles L.1111-8 et L.1111-14 et suivants du Code de la santé publique.
[59] La directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sera abrogée en date du 25 mai 2018 par le RGPD.

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.

En ce qui concerne spécifiquement le traitement de catégories particulières de données à caractère personnel, le considérant (54) du RGPD reconnaît des hypothèses dans lesquels le traitement de catégories particulières de données à caractère personnel (données dites « sensibles ») *« peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. Un tel traitement devrait faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques ».*

En effet, outre l'hypothèse d'un consentement explicite de la personne (article 9 paragraphe (2) lettre a) du RGPD), plusieurs situations peuvent légitimer un traitement portant sur des catégories particulières de données à caractère personnel, en particulier des données de santé. C'est notamment le cas lorsque *« le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel »* (article 9 paragraphe (2) lettre i) du RGPD), ou encore lorsque *« le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée »* (article 9 paragraphe (2) lettre g) du RGPD).

La Commission nationale estime que les traitements de données mis en œuvre au moyen d'un DSP activé d'office, avec possibilité pour le titulaire de s'y opposer, pourraient relever des motifs d'intérêt public important, et plus spécifiquement des motifs d'intérêt public dans le domaine de la santé publique visés à l'article 9 paragraphe (2) lettres i) et g) du RGPD susmentionné du RGPD, à condition que le droit national le prévoit et que cette législation prévoit de telles *« mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée ».*

L'article 6 paragraphe (3) du RGPD 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 ».*

Le considérant (45) du RGPD précise qu'il devrait « *[…] appartenir au droit de l'Union ou au droit d'un État membre de déterminer la finalité du traitement. Par ailleurs, ce droit pourrait préciser les conditions générales du présent règlement régissant la licéité du traitement des données à caractère personnel, établir les spécifications visant à déterminer le responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal. […] ».*

Le considérant (41) énonce encore que *« cette base juridique ou cette mesure législative 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. »*

Ainsi, la Commission nationale se doit de souligner 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 »*[60]. 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 »*[61]. *« Le degré de précision requis de la « loi » à cet égard dépendra du sujet en question. »*[62]

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*

[60] 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.

[61] 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.

[62] 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.

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. »[63]

Le Conseil d'État 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 (…). »[64]

Si on se réfère donc à l'article 9 paragraphe (2) lettres i) et g) du RGPD comme base légale, il y a lieu de vérifier si le droit luxembourgeois prévoit des « mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée » telles qu'exigées par le RGPD. A cet égard, la CNPD avait déjà fait remarquer dans son avis n° 345/2010 précité que *« l'introduction d'un système généralisé de dossiers électroniques partagés répond au critère posé à l'article 8 paragraphe 4 de la directive 95/46/CE*[65] *dès lors que le projet de loi [n° 6196 portant réforme du système de soins de santé] apporte les garanties appropriées suffisantes en matière de protection de la vie privée et des données personnelles ».*

Or, suite à l'adoption du projet de loi n° 6196 susmentionné, l'article 60quater du Code de la sécurité sociale renvoie à un règlement grand-ducal afin de préciser les garanties prévues dans le cadre du DSP. A cet égard, il conviendra de veiller à une application rigoureuse des principes d'encadrement normatif susmentionnés s'agissant de la distinction entre ce qui doit relever, par essence, de la loi au sens stricte et ce qui peut faire l'objet d'un encadrement normatif par un texte réglementaire. La CNPD considère ainsi qu'au moins les dispositions concernant la durée de conservation des données au DSP, figurant actuellement aux articles 4 paragraphes (2) à (5) et 10 paragraphe (5) du projet, les dispositions réglementant les droits des titulaires mineurs non émancipés et titulaires majeurs protégés par la loi (actuel article 7 du projet), ainsi que la limitation du droit d'accès telle que prévue par l'article 9 paragraphe (2) et la limitation du droit à l'effacement (article 6)du projet devraient être prévues dans la loi au sens stricte du terme et plus précisément par l'article 60quater du Code de la sécurité sociale, et non pas dans un acte réglementaire. Elle reviendra sur ces différents points plus loin dans le présent avis.

b. <u>La question de la responsabilité du traitement</u>

L'article 60ter (4) du Code de la sécurité sociale prévoit que l'Agence nationale des informations partagées dans le domaine de la santé (ci-après désignée « l'Agence eSanté ») a la qualité de responsable du traitement des données à caractère personnel au sens de la loi modifiée du 2 août 2002.

[63] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015

[64] Voir par exemple : Conseil d'État, 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'État pour études supérieures.

[65] Son article 8 paragraphe 4 dispose que *« sous réserve de garanties appropriées, les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues au paragraphe 2, soit par leur législation nationale, soit sur décision de l'autorité de contrôle. »*

En ce qui concerne précisément les questions de responsabilité, le groupe de travail « article 29 » a précisé que *« tout système de DME [dossiers médicaux électroniques] doit également garantir que le risque d'atteintes à la vie privée dû au stockage de données médicales et à la fourniture de ces données soit adéquatement contrebalancé par la responsabilité pour le préjudice causé, par exemple par l'utilisation incorrecte ou non autorisée de données des DME.* » Il a recommandé aux États membres désirant instaurer un système de DSP de *« mener minutieusement au préalable des études approfondies de droit civil et médical réalisées par des experts et des évaluations d'impact pour clarifier les nouvelles questions de responsabilité susceptibles de se poser dans ce contexte, notamment en ce qui concerne l'exactitude et l'exhaustivité des données inscrites dans le DME, la définition du degré de connaissance qu'un professionnel de santé traitant un patient doit avoir du DME de celui-ci ou les conséquences prévues par le droit de la responsabilité si l'accès est indisponible pour des raisons techniques, etc. »*[66]

Or, la CNPD considère que la responsabilité unique de l'Agence eSanté concernant les traitements des données à caractère personnel contenues dans le DSP ne correspond pas à la réalité tel que le système est envisagé. En effet, déjà dans son avis relatif au projet de loi n° 6196 portant réforme du système de soins de santé, la CNPD a estimé qu'il résulte de l'économie générale dudit projet de loi que la responsabilité est exercée de manière conjointe.

Ainsi, tout professionnel de santé qui consulte un DSP est tenu de traiter les données de manière loyale et licite et dans le respect des finalités légales du traitement tel que prévu par l'article 5 paragraphe (1) lettres a) et b) du RGPD.

Ensuite, le professionnel de santé qui inscrit des informations dans un DSP est tenu de vérifier l'exactitude de ses informations et il doit s'astreindre à intégrer uniquement les données *« utiles et pertinentes*[67] *»*. L'article 5, paragraphe (1), lettres (c) et (d) du RGPD précise que les données à caractère personnel doivent être *« adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) (et) exactes et, si nécessaire, tenues à jour […] ».*

Pour sa part, le médecin référent se voit attribuer un rôle plus important dans le fonctionnement du DSP. Ses missions sont plus nombreuses que celles qui incombent aux différents intervenants isolés. L'article 19bis du Code de la sécurité sociale précise que le médecin référent a notamment pour mission de *« 3) suivre régulièrement le contenu du dossier de soins partagé de l'assuré […] ».* L'article 8 paragraphe (2) alinéa 2 du projet de règlement grand-ducal prévoit d'ailleurs que le médecin référent est présumé intervenir dans la prise en charge du titulaire pendant la durée de relation patient médecin référent et de ce fait, il peut d'office accéder au DSP de ses patients et y verser des données.

Le groupe de travail « Article 29 » suggère par ailleurs qu'une seule personne soit responsable envers les patients de l'usage correct des demandes d'accès : *« Les systèmes de DME sont toutefois des systèmes de mise en*

[66] Document de travail (WP 131) sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007, p. 23.
[67] Article 60*quater* paragraphe (2) du Code de la Sécurité sociale.

commun d'informations qui comptent de nombreux responsables du traitement des données. Dans ces conditions, une seule institution spéciale doit être responsable envers les personnes concernées du traitement correct des demandes d'accès. Vu la complexité prévisible d'un DME pleinement opérationnel et la nécessité de faire en sorte que les patients aient confiance dans le système, il semble essentiel que les patients dont les données sont traitées dans un DME sachent comment contacter un partenaire responsable avec lequel ils peuvent discuter des éventuelles lacunes du système. Des dispositions spéciales à cet effet devront être incluses dans tout règlement sur les systèmes de DME. »[68]

Enfin, l'Agence eSanté a une responsabilité particulière en matière de sécurité du système en étant chargée notamment d'une mission technique et administrative pour mettre en place l'architecture technique et organisationnelle du dossier de soins partagé.

La Commission nationale note par ailleurs que les différents intervenants doivent en tout état de cause, chacun pour ce qui le concerne, assumer les obligations prévues à l'article 32 du RGPD en matière de sécurité du traitement.

La notion de « responsabilité conjointe » introduite par le RGPD est à prendre en compte dans ce contexte, la Commission nationale étant d'avis qu'il ressort de l'économie générale de la loi du 17 décembre 2010 portant réforme du système de soins de santé que l'Agence eSanté d'un côté, et les professionnels de santé d'autre côté, participent conjointement à la réalisation des finalités et des moyens du traitement tels que définis par le législateur. L'article 26 paragraphe (1) du RGPD exige que *« les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. »*

Or, dans la mesure où le texte prévoit par exemple à l'article 6 paragraphe (5) que la rectification des données inexactes ou incomplètes dans un DSP peut être sollicitée par un titulaire auprès du professionnel de santé auteur de la donnée et non pas auprès de l'Agence eSanté, les droits des personnes concernées ne s'exercent pas exclusivement auprès du responsable du traitement, c'est-à-dire auprès de l'Agence eSanté. La Commission nationale renvoie dans ce contexte à ses commentaires sous le point *« VI. Droits d'accès, d'écriture et d'opposition du titulaire ».*

Sur base des considérations ci-dessus, la CNPD est d'avis que l'article 60*ter* (4) du Code de la sécurité sociale devrait être modifié afin de prévoir les responsabilités des différents acteurs.

[68] Pages 23 et 24 du document de travail WP 131.

c. La question des sanctions

Dans son avis relatif au projet de loi n° 6196 portant réforme du système de soins de santé, la CNPD avait critiqué le manque de précision quant à la responsabilité des différents intervenants du DSP et quant aux éventuelles sanctions :

« En définitive, 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 dossier de soins partagé. Or, en cas de non-respect des différentes obligations légales, le texte sous examen ne règle pas la question de la responsabilité. Notons que la loi du 2 août 2002 prévoit des sanctions pénales à l'égard du responsable du traitement. »[69]

En France, des sanctions pénales sont prévues en cas de manquement aux dispositions du Code de la santé publique concernant l'accès au dossier médical partagé.[70]

En ce qui concerne précisément les sanctions pénales, 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 ».*

Ainsi, la CNPD profite de l'occasion pour réitérer sa recommandation émise dans le cadre de son avis relatif au projet de loi n° 7184 portant création de la CNPD et la mise en œuvre du RGPD qu'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 n° 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*

[69] Délibération 345/2010 du 24 novembre 2010, p.5.
[70] Article L1111-18, alinéa 4 du Code de la santé publique.

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). »

Ainsi, la CNPD estime qu'à l'instar du Code de la santé publique français la législation luxembourgeoise devrait prévoir des sanctions pénales en cas d'abus d'accès au DSP.

XI. La création du dossier de soins partagé

A titre liminaire, la CNPD voudrait remarquer qu'en fournissant une définition du terme « patient », le commentaire relatif à l'article 1ier point 4 ne concorde pas avec la définition prévue audit point 4 concernant le terme « titulaire ». Ainsi, les auteurs du projet devraient analyser la pertinence de l'ajout de la définition du terme « patient » dans l'article 1ier du projet.

La Commission nationale s'interroge par ailleurs sur les catégories de données contenues dans le DSP lors de sa création / activation.

Selon l'article 1ier point 3° lettre b) de la loi du 13 décembre 2017 modifiant certaines dispositions du Code de la sécurité sociale, le paragraphe 2 de l'article 60*ter* du Code de la sécurité sociale est complété, entre autres, par les alinéas suivants :

« L'annuaire référentiel d'identification des patients comprend les données d'identification, les caractéristiques personnelles et la situation de famille du patient ainsi que les noms, prénoms, adresses et numéros d'identification des représentants légaux des mineurs d'âge non émancipés et des personnes majeures protégées par la loi.

[…]

L'annuaire référentiel d'identification des prestataires de soins comprend les données d'identification et les données en relation avec la profession et l'emploi du prestataire. »

Néanmoins, la Commission nationale se pose la question si les données issues de ces annuaires seront aussi intégrées dans les DSP ? Dans l'affirmative, les catégories de données inclues dans lesdits annuaires devraient être ajoutées à celles déjà prévues à l'annexe 1 du projet de règlement grand-ducal sous le numéro (2).

L'article 2 paragraphe (1) du projet prévoit ensuite que l'assuré est informé par le Centre commun de la sécurité sociale de la création d'un DSP par l'Agence eSanté, sans précisant à quel moment cette information aura lieu et sur quoi elle porte. La CNPD s'interroge à quel titre le Centre commun de la sécurité sociale intervient dans la mesure

où l'obligation d'information incombe au responsable du traitement, c'est-à-dire à l'Agence eSanté. N'y a-t-il pas une incohérence entre le paragraphe (1) et le paragraphe (3) de l'article 2 ?

En vertu de l'article 2 paragraphe (2) du projet de règlement grand-ducal, le patient non affilié bénéficiant de soins de santé par un prestataire de soins établi au Luxembourg, peut demander l'ouverture d'un DSP moyennant un formulaire de demande à adresser à l'Agence eSanté. Le commentaire des articles précise à cet égard que ledit formulaire doit être accompagné des *« pièces justificatives nécessaires »*. La CNPD considère que cette catégorie de données manque de clarté et de précision et elle estime nécessaire de décrire de manière plus précise et concise ces *« pièces justificatives nécessaires »* dans le corps du texte. En effet, s'agissant d'une collecte de données et au regard du principe de proportionnalité et de nécessité (principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre c) du RGPD), la CNPD n'est pas en mesure d'apprécier si ce principe est respecté.

L'article 2 paragraphe (3) du projet quant à lui oblige l'Agence eSanté à fournir certaines informations aux titulaires dès la création du DSP. Or, la liste des informations à communiquer aux personnes concernées a été allongée par rapport à la loi modifiée du 2 août 2002, respectivement à la directive européenne 95/46 du 24 octobre 1995, en vertu des articles 13 et 14 du RGPD (applicables à partir du 25 mai 2018), dépendant du fait si les données ont été collectées directement auprès de la personne concernée ou non.

Ainsi, il est important de préciser qu'à côté des informations prévues à l'article 2 paragraphe (3) du projet, l'Agence doit prendre en considération les listes d'informations obligatoires prévues aux articles 13 et 14 du RGPD. Elle doit par exemple informer les titulaires sur les finalités précises du DSP, les coordonnées du délégué à la protection des données, sur les destinataires ou les catégories de destinataires des données à caractère personnel, sur la durée de conservation des données à caractère personnel, ainsi que sur le droit d'introduire une réclamation auprès de la CNPD. De même, il parait utile d'informer les titulaires sur le contenu précis du DSP lors de son activation.

Finalement, l'exposé des motifs précise que *« le dossier de soins partagé ne se substitue pas au dossier individuel du patient que tout prestataire de soins doit obligatoirement tenir. »* La Commission nationale estime que cette précision devrait figurer dans le texte même du règlement grand-ducal en projet. Dans le cas où il serait tenu compte de cette suggestion de la CNPD, cette précision pourrait figurer dans un paragraphe (4) nouveau de l'article 2 du projet.

XII. <u>L'activation du dossier de soins partagé et accès par le titulaire</u>

L'article 3 paragraphe (1) du projet précise que pour accéder à son DPS, le titulaire est obligé d'activer au préalable un compte sur la plateforme et de se connecter par après à l'application moyennant les identifiants de connexion

lui envoyés par l'Agence eSanté selon l'article 2 paragraphe (3) lettre c) du projet. Or, le commentaire des articles indique que *« le titulaire doit lui-même activer son compte sur la plateforme pour recevoir ses identifiants de connexion »*. Néanmoins, lors de l'activation de son compte sur la plateforme, le titulaire devrait en principe déjà disposer de ses identifiants de connexion ?

De même, il ne ressort pas clairement du texte ce que les auteurs du projet entendent par « plateforme ». Ce n'est que si on lit la définition de la notion « Application dossier de soins partagé » (article 1ier, point 2 du projet) qu'on comprend qu'il s'agit de la plateforme électronique nationale d'échange et de partage de données de santé visée à l'article 60*ter* du Code de la sécurité sociale. Pour des raisons de compréhension, la CNPD suggère de préciser dans l'article 3 du projet que le DSP est accessible aux professionnels de santé, ainsi qu'à son titulaire, par voie électronique depuis un site internet.

Par ailleurs, en lisant l'article 3 paragraphe (3) du projet, on a l'impression qu'à défaut d'activation dans les 30 jours suivant l'envoi des informations visées à son article 2 paragraphe (3), le DSP peut exclusivement être consulté et alimenté par les professionnels de santé, et non plus par son titulaire. Le commentaire des articles précise toutefois que le titulaire peut, même après l'écoulement de ce délai, accéder à son DSP en procédant à son activation et à la configuration de son compte sur la plateforme.

Le commentaire des articles énonce dans ce même contexte qu'afin *« d'éviter la création de dossiers de soins partagés non utilisables par les professionnels de santé faute de création active d'un compte par les titulaires, il est prévu d'instaurer une période dite « blanche » au-delà de laquelle, à défaut d'activation du compte par son titulaire, le dossier devient* ***automatiquement fonctionnel pour les professionnels de santé.*** *»*

Or, même sans activation de compte par un titulaire sur la plateforme, la CNPD a pu comprendre qu'en vertu de l'article 8 paragraphe (2) du projet, un professionnel de santé peut uniquement accéder ou alimenter un DSP d'un titulaire dans le cadre d'une prise en charge documentée, à l'exception du médecin référent qui peut y accéder à tout moment. Ou est-ce que le fait que le DSP *« devient automatiquement fonctionnel pour les professionnels de santé »* implique que ces derniers pourront en dehors du cadre d'une prise en charge, suivant la matrice des accès d'habilitation par défaut, consulter et alimenter le DSP d'une personne qui pour une raison ou une autre n'aura pas pu prendre connaissance de la création de son DSP ?

La CNPD est ainsi d'avis que les auteurs du projet devraient au moins prévoir que le titulaire qui n'aura pas encore activé son DSP recevra une deuxième information lors du premier accès à son DSP par un professionnel de santé. Elle renvoie dans ce contexte également à ses observations formulées au point *« VIII. Droits d'accès et d'écriture des professionnels de santé »*.

XIII. Fermeture et suppression du dossier de soins partagé

L'article 4 du projet accorde la possibilité au titulaire de fermer son DSP à tout moment, soit via l'application DSP, soit par demande à adresser à l'Agence eSanté.

La CNPD renvoie à ses commentaires sous le point *« I. Remarques préliminaires »* en ce qui concerne l'intégration des dispositions concernant la durée de conservation des données au DSP dans une loi, c'est-à-dire dans l'article 60quater du Code de la sécurité sociale et non pas dans un acte réglementaire.

A l'instar de l'article L.1111-18 du Code de la santé publique français, les données du DSP sont supprimées dix ans après sa fermeture par le titulaire. Pendant ce laps de temps et selon le commentaire des articles, les données versées au DSP deviennent inaccessibles au titulaire, ainsi qu'aux professionnels de santé. *« Toutefois, en vue de permettre ultérieurement non seulement au titulaire d'exercer son droit d'accès à ses données à travers l'Agence et la traçabilité des actions passées mais également afin de lui donner la possibilité de rouvrir son dossier sans perte préjudiciable pour sa bonne prise en charge au regard de la finalité du dossier de soins partagé, il est prévu de conserver les données pendant une durée de dix ans à partir de la fermeture. »*[71]

La CNPD considère néanmoins qu'une durée d'archivage intermédiaire des données de dix ans apparaît comme excédant celle nécessaire au regard des finalités d'exercice du droit d'accès et d'une éventuelle réouverture du DSP. En effet, le DSP n'a pas vocation à se substituer aux dossiers des patients tenus par les médecins, établissements hospitaliers et autres professionnels de santé.

Par ailleurs, si on se réfère à l'avis des praticiens, c'est-à-dire aux professionnels de santé et en particulier à l'avis de l'Association des médecins et médecins-dentistes (ci-après : « l'AMMD »), cette durée de conservation ne correspondrait pas à la réalité des moyens et de l'utilité de la profession, alors qu'ils estiment qu'un professionnel de santé ne serait pas en mesure de consulter les données sur une période de dix ans. L'AMMD insiste sur le fait que la finalité de partage et d'échange de données ne soit pas détournée en une finalité de stockage ou d'archivage des données de santé contenues dans le DSP. Suivant l'adage « trop d'information tue l'information », elle est d'avis qu'un *« temps de conservation de 5 ans ou au-delà ne fera que saturer le DSP de documents inutiles voire obsolètes rendant ainsi laborieuse la consultation du DSP par les médecins et les autres prestataires de santé. »*[72]

Sur base des considérations ci-dessus, la CNPD estime qu'une durée de conservation des données de cinq ans suite à une fermeture d'un DSP respecte le principe de la limitation de conservation prévu par l'article 5 paragraphe (1) lettre e) du RGPD, selon lequel des données à caractère personnel doivent uniquement être *« conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. »*

[71] Commentaire de l'article 4 du projet de règlement grand-ducal.
[72] Avis de l'AMMD du 11 juillet 2017 au sujet du DSP et la durée de conservation des documents qui y sont attachés.

La CNPD renvoie aussi à ses observations sous le point X *« Délai de versement des données au dossier de soins partagé »* concernant l'appréciation de la durée de conservation des données dans le DSP en dehors du contexte d'une fermeture par le titulaire.

Par ailleurs, le paragraphe (3) de l'article 4 du projet énonce que les *« données du DSP sont supprimées »* dix ans après la fermeture du DSP à défaut de réouverture endéans ce délai. La CNPD estime néanmoins que non seulement les données doivent être supprimées du DSP, mais que le DSP en lui-même doit être supprimé intégralement.

La CNPD partage également la position de la CNIL exprimée dans son avis relatif au projet de décret en Conseil d'État autorisant la création d'un traitement de données à caractère personnel dénommé « dossier médical partagé »[73] en ce sens qu'elle recommande qu'en cas de clôture d'un DMP *« son titulaire soit informé que les données qu'il contient ne seront plus accessibles. Une telle information apparaît d'autant plus pertinente quand le DMP contient des données particulières telles que les directives anticipées du titulaire. Dans cette hypothèse, le titulaire pourrait, par exemple, être invité à recourir à l'un des autres modes de dépôt prévus pour les directives anticipées »*. Dans le cadre de ce projet, cette recommandation est aussi valable en ce qui concerne les volontés du titulaire en matière de don d'organes au sens de l'article 6 paragraphe (2) lettre b) du projet.

Finalement, la CNPD estime nécessaire de clarifier dans le projet quelles sont les modalités d'exercice des droits d'accès spécifiques au DSP d'une personne décédée et si, le cas échéant, ces accès s'exerceront conformément à l'article 19 de la loi du 24 juillet 2014 relative aux droits et obligations du patient.

XIV. Accès au dossier de soins partagé par les professionnels de santé

L'article 5 du projet règlemente l'accès au DSP par les professionnels de santé. Il ressort de son paragraphe (1) qu'afin d'accéder au DSP de ses patients, le professionnel de santé doit au préalable créer un compte sur la plateforme. Ce compte ne sera créé par l'Agence eSanté que sur demande explicite, soit d'un professionnel de santé individuel, soit d'une collectivité de santé. Un professionnel de santé a donc la possibilité de ne pas faire de telle demande et de refuser d'utiliser le DSP ? La CNPD constate donc qu'il y aura un système « d'opt-out » pour les patients, tandis que pour les professionnels de santé un système « d'opt-in » s'appliquera.

Notons encore que les auteurs du projet ne définissent pas la notion de « collectivité de santé ». Le commentaire de l'article 9 du projet se contente d'expliquer qu'il s'agit par exemple des établissements hospitaliers, laboratoires, des centres d'aide et de soins, etc.

[73] Délibération no 2016-258 du 21 juillet 2016 de la Commission nationale de l'informatique et des libertés portant avis sur un projet de décret en Conseil d'État autorisant la création d'un traitement de données à caractère personnel dénommé « dossier médical partagé » (demande d'avis no 16017107).

XV. Droits d'accès, d'écriture et d'opposition du titulaire

L'article 6 du projet encadre les droits d'accès, d'écriture et d'opposition du titulaire. Pour ce qui est plus particulièrement du paragraphe (3), la CNPD a l'impression que la lettre b) se trouve en contradiction avec la lettre d) dans la mesure où d'abord le droit est accordé au titulaire de rendre inaccessible certaines données spécifiques aux professionnels de santé, *« à l'exception de son médecin référent et des professionnels d'un service d'urgence d'un établissement hospitalier »*, alors qu'il lui est aussi accordé possibilité de refuser *« aux professionnels de santé d'un service d'urgence d'un établissement hospitalier l'accès aux données de niveau « restreint » ou en leur refusant l'accès à son dossier de soins partagé »*. Cette dernière hypothèse apparaît en elle-même contradictoire par rapport à son commentaire des articles qui énonce que *« le masquage peut être appliqué envers tout professionnel de santé (niveau privé) ou simplement envers certains d'entre eux (niveau restreint), à condition, dans ce dernier cas, qu'il ne s'agisse pas du médecin référent ou, sauf masquage étendu, d'un professionnel de santé d'un service d'urgence d'un établissement hospitalier. »*

Le groupe de travail européen « article 29 » a précisé dans ce contexte que même si un système de DSP n'a pas uniquement le consentement pour base juridique, *« la détermination par le patient lui-même de quand et comment ses données sont utilisées devrait constituer une garantie majeure »*.[74] L'autodétermination informationnelle du patient joue donc un rôle central au niveau de trois stades successifs : lors de la création du DSP, lors de l'inscription des données dans le DSP, ainsi que lors de la consultation du DSP par les professionnels de santé.

Par ailleurs, il ressort implicitement de l'article 6 du projet que le titulaire peut, soit s'opposer directement au préalable lors de sa prise en charge au versement de données dans son DSP, soit rendre inaccessible par le masquage une donnée spécifique aux professionnels de santé. A contrario, le titulaire ne dispose pas du droit de demander a posteriori la suppression d'une donnée de son DSP qu'il juge particulièrement sensible. Est-ce que le contrôle du titulaire sur ses données de santé ne devrait-il pas inclure cette possibilité de pouvoir supprimer (et non seulement masquer) un document de santé, d'autant plus que le médecin traitant aura toujours accès à ce document qui se trouvera dans son dossier patient ?

En ce qui concerne une limitation des droits des personnes concernées, comme notamment le droit à l'effacement (« droit à l'oubli »), l'article 23 paragraphe (1) du RGPD dispose que le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter, entre autres, la portée du droit à l'effacement prévu par l'article 16 du RGPD. Une telle limitation doit respecter l'essence des libertés et droits fondamentaux et elle doit constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des dix motifs y prévus. Une mesure législative limitative doit d'ailleurs contenir certaines dispositions spécifiques énumérées à l'article 23 paragraphe (2) du RGDP.

[74] Document de travail (WP 131) sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007, p. 15

Ainsi, comme l'article 6 du projet sous examen limite implicitement le droit à l'effacement des titulaires d'un DSP, cette limitation doit être prévue par une loi au sens stricte du terme et respecter les exigences susmentionnées prévues à l'article 23 du RGPD.

Pour ce qui est précisément de la faculté pour le titulaire de rendre inaccessible *« certaines données spécifiques aux professionnels de santé […] »*, la CNPD estime que cette possibilité ne correspond pas à la réalité du système tel qu'il est conçu et elle se demande notamment comment concrètement l'Agence eSanté en tant que responsable du traitement entend faire droit à de telles requêtes. En effet, le DSP ne contient que peu de données individuelles ou structurées, mais se compose en réalité et surtout de documents scannés, chaque document contenant une multitude d'informations ou données de santé relatives à un patient.

LA CNPD est dès lors à se demander comment il pourra être garanti qu'un titulaire puisse rendre inaccessible « certaines données spécifiques » (par exemple des données relatives à une interruption volontaire de grossesse) contenues dans plusieurs documents médicaux scannés. A moins de rendre inaccessible l'intégralité de documents, elle est d'avis qu'il ne sera pratiquement pas possible de « masquer » ou d'isoler certaines données spécifiques dans l'ensemble des documents contenant ces données spécifiques.

Il y a donc lieu de constater que le texte du règlement grand-ducal en projet ne reflète pas la réalité, de sorte que les dispositions en question, pourtant fondamentales en termes de protection des données et de la vie privée, risquent de ne pas pouvoir être appliquées en pratique.

Le paragraphe (5) de l'article 6 prévoit finalement que la rectification des données inexactes ou incomplètes dans son DSP peut être sollicitée par le titulaire auprès du professionnel de santé auteur de la donnée. Or, l'article 16 du RGPD dispose que la *« personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. »* En application du RGPD et du Code de la Sécurité sociale, la demande de rectification des données devrait être adressée par le titulaire à l'Agence eSanté en sa qualité de responsable du traitement.

A ce titre il est encore renvoyé aux observations faites au point *« I.c »* du présent avis relatif à la question du responsable du traitement du DSP, respectivement d'une responsabilité conjointe de l'Agence eSanté et des professionnels de santé.

XVI. <u>Titulaires mineurs non émancipés et titulaires majeurs protégés par la loi</u>

L'article 7 du projet réglemente les droits des titulaires mineurs non émancipés et titulaires majeurs protégés par la loi. A titre préliminaire, quant à la forme la CNPD tient à souligner que l'article 7 déroge aux dispositions du Code civil. En effet, alors que l'article 7 paragraphe (1) alinéa 2 du projet accorde un droit de consultation au DSP au mineur âgé de 16 ans et plus (ou âgé de moins de 16 ans en cas de demande de son ou ses représentants

légaux), l'article 488 du Code civil prévoit que la majorité est fixée à dix-huit ans accomplis et que ce n'est qu'à cet âge qu'une personne est capable de tous les actes de la vie civile. En ce qui concerne les majeurs protégés par la loi, des procédures spécifiques sont prévues aux articles 491 à 515 du Code Civil.

Or, en vertu du principe de la hiérarchie des normes, un acte réglementaire ne peut déroger à une loi. La CNPD estime dès lors nécessaire de prévoir les dispositions en question dans une loi.

Ceci dit, la Commission nationale voudrait formuler les observations suivantes quant au fond. Le considérant (58) du RGPD précise que les enfants méritent une protection spécifique et ainsi *« toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre. »*

Selon l'article 12 paragraphe (1) du RGPD, le responsable du traitement doit prendre des mesures appropriées pour fournir toute information ou procéder à toute communication au titre des articles 13 à 22 et 34 du RGPD et ceci d'une *« façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. »*

L'article 7, paragraphe (2) du projet sous examen prévoit que les informations prévues à l'article 2 paragraphe (3) du projet sont, en sus d'être adressées aux représentants légaux du titulaire mineur non émancipé, également transmises au mineur âgé de 16 ans ou plus et, en cas de demande de son ou ses représentants légaux, au mineur âgé de moins de 16 ans. Ainsi, la CNPD se demande s'il ne faudrait pas prévoir des feuillets d'information spécifique désignés aux mineurs en cause conformément au RGPD.

Par ailleurs, l'article 7 paragraphe (1) alinéa 3 du projet accorde la possibilité au titulaire mineur non émancipé de s'opposer au versement des données liées à une interruption volontaire de grossesse à son DSP. Or, la CNPD se demande pourquoi les auteurs ont choisi de limiter le projet à ce cas spécifique ? Elle suggère d'utiliser la formulation plus large du commentaire des articles prévoyant que ledit mineur peut *« dans les cas légalement prévus »* demander au professionnel de santé de ne pas introduire une donnée à son DSP afin de la garder confidentielle envers son ou ses représentants légaux.

Finalement, afin de respecter l'autodétermination informationnelle des mineurs devenus majeurs, la CNPD demande que la désactivation des identifiants de connexion personnels des représentants légaux au DSP du mineur devenu majeur s'opère de manière automatique.

XVII. Droits d'accès et d'écriture des professionnels de santé

Les droits d'accès et d'écriture des professionnels de santé sont prévus par l'article 8 du projet.

Son paragraphe (1) renvoie à la matrice d'accès figurant à l'annexe 1 du projet en ce qui concerne les *« les droits d'accès et d'écriture maximaux par catégorie de données des professionnels de santé intervenant dans la prise en charge du titulaire ».*

En vertu de l'article 25 paragraphe (2) du RGPD, le responsable du traitement doit mettre *« en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées »* (principe du « Privacy by Default »). Ledit article précise qu'en *« particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. »* Une matrice des accès par défaut, comme celle prévue à l'annexe 1 du projet sous examen, doit par principe être considérée comme étant contraire audit principe du « Privacy by Design ».

L'alinéa 2 du paragraphe (1) de l'article 8 du projet de règlement grand-ducal précise que ledit classement, ainsi que *« d'éventuelles restrictions d'accès et d'écriture à certains types de données à l'intérieur d'une même catégorie de données se font conformément aux procédures déterminées par l'Agence. »* Or, la Commission nationale est d'avis que le texte du règlement grand-ducal doit préciser quelles sont ces procédures.

Le paragraphe (2) de l'article 8 du projet prévoit des modalités spécifiques pour le *« classement d'un type de donnée au sein d'une catégorie de données »*. En se référant à ses commentaires sous le point « VI. Droits d'accès, d'écriture et d'opposition du titulaire » et en tenant compte du fait que figurent au sein du DSP surtout des documents scannés qui ne présentent aucune granularité, la CNPD rappelle que le texte du projet ne correspond pas à la réalité de la configuration des systèmes mis en place. Elle se demande notamment comment l'Agence eSanté en tant que responsable du traitement va maîtriser la situation dans laquelle plusieurs catégories de données se retrouvent dans un même document scanné et qu'un professionnel de santé n'a droit d'accéder uniquement à une catégorie, mais non pas à l'autre ?

Selon l'article 8 paragraphe (2) du projet, uniquement les professionnels de santé intervenant dans la prise en charge du titulaire peuvent y accéder selon la matrice des accès par défaut annexée au projet sous examen. Le but du DSP est précisément de regrouper à des fins de partage des données de santé d'un patient nécessaires pour lui assurer un meilleur suivi par les professionnels de santé qui s'occupent de lui. Il ressort ainsi implicitement de cet article que les données de santé contenues dans le DSP ne peuvent pas être utilisées pour d'autre fins, en excluant ainsi l'accès au DSP par *« des praticiens de la médecine qui agissent en tant qu'experts pour le compte de tiers: par exemple pour des compagnies d'assurance privées, dans des litiges, pour l'octroi de l'aide à la retraite, pour les employeurs de la personne concernée, etc. »*[75]

Déjà dans son avis n° 345/2010 précité, la CNPD avait estimé, dans le souci du respect des finalités pour lesquelles le DSP est institué, que la liste des destinataires ne devrait pas être élargie à l'avenir à d'autres catégories

[75] Document de travail (WP 131) sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007, p. 18.

de personnes. Elle avait renvoyé dans ce contexte à l'article L1111-18 du Code français de la santé publique qui dispose ce qui suit : *« l'accès au dossier médical partagé est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application. »*

Ainsi, la CNPD rappelle qu'il est primordial d'inclure une telle disposition dans une loi, sinon dans le texte du projet de règlement grand-ducal sous avis.

Le paragraphe (2) de l'article 8 du projet, en limitant l'accès au DSP aux seuls professionnels de santé intervenant dans la prise en charge du titulaire, parait par ailleurs en contradiction avec l'article 10 paragraphe (1) du projet, en ce sens qu'il autorise tout professionnel de santé, sans distinction s'il intervient dans la prise en charge du titulaire ou non à verser toute donnée qu'il détient et qu'il estime utile et pertinente au DSP *« dans un délai raisonnable après la prise de connaissance de cette donnée ou après son premier accès au dossier de soins partagé si cette donnée est antérieure à son activation. »* La CNPD renvoie à ce titre à ses commentaires sous le point *« X. Délais de versement des données au dossier de soins partagé ».*

L'article 8 paragraphe (4) du projet permet au prestataire de santé d'inclure une information dans un DSP qui sera temporairement inaccessible au titulaire jusqu'à ce qu'une consultation médicale avec ce dernier aura lieu. Comme cette possibilité se trouve en contradiction avec la philosophie générale du DSP où le contrôle réside auprès du titulaire, la CNPD est d'avis que cette faculté devrait être strictement encadrée et limitée au cas strictement nécessaires et proportionnels.

Dans son avis précité, la Commission consultative statutaire « aspects éthiques et déontologiques en relation avec la protection et l'accessibilité des données » a estimé que la possibilité d'un masquage ciblé de documents devrait être offerte aux professionnels de santé désireux de procéder à une consultation d'annonce de leur contenu, sous condition *« de prévoir en tant que garde-fous […] la levée automatique du masquage après l'écoulement d'un délai raisonnable (par exemple de six semaines). »*

C'est précisément ce que le législateur français a prévu, alors que l'article R1111-42 du Code de la santé publique prévoit que *« dans un délai de deux semaines suivant le versement d'une information inaccessible, et en l'absence de la consultation d'annonce, le patient est informé par tout moyen y compris dématérialisé d'une mise à jour de son dossier médical partagé, l'invitant à consulter un professionnel de santé, notamment son médecin traitant, pour en prendre connaissance. Si la consultation d'annonce n'a pas eu lieu un mois après le versement de l'information dans le dossier médical partagé du patient, elle devient automatiquement accessible. »* Ainsi, la CNPD estime nécessaire que les auteurs précisent une telle durée limitée de masquage dans le projet de règlement grand-ducal.

Par ailleurs, il ressort de l'article 8 paragraphes (2) et (3) du projet, ainsi que du commentaire des articles, que contrairement aux professionnels de santé exerçant dans un cabinet médical privé, ceux qui interviennent dans une collectivité de santé ou dans un service d'urgence n'ont pas besoin de recevoir au préalable, lors de l'acte ou de la consultation, l'identifiant de connexion du titulaire, mais peuvent directement y accéder. Bien sûr, le commentaire des articles précise qu'un *« titulaire a toujours le droit de s'opposer à l'accès soit au moment de son admission soit moyennant configuration dans son DSP ».* Cette différence de traitement est justifiable en ce qui concerne les services d'urgence, le titulaire n'étant souvent pas en état de fournir ses identifiants. Or, qu'en est-il de la différence de traitement entre les professionnels de santé exerçant dans un cabinet médical privé et ceux qui interviennent dans une collectivité de santé ? Comment « la prise en charge », qui n'est d'ailleurs pas définie, est-elle constatée ou documentée par une « collectivité de santé » (qui n'est pas non plus définie par le texte en projet), étant donné que le patient ne donne pas son identifiant de connexion à la collectivité de santé pour manifester son accord à l'accès de son DSP ? Autrement dit, comment le patient peut-il savoir qu'une collectivité de santé (par exemple un laboratoire, un centre d'aide et de soins, etc.) va accéder à son DSP et qu'il a la possibilité de refuser l'accès à son DSP, s'il n'en a pas conscience ou s'il n'en est pas informé ? Le texte du projet reste muet à ce sujet, alors qu'il ne prévoit aucune obligation pour une collectivité de santé d'informer le patient en ce sens au moment de la prise en charge.

La CNPD doit dès lors insister que le règlement grand-ducal prévoit une disposition qui oblige une collectivité de santé d'informer le patient qu'elle entend accéder à son DSP et qu'il a la possibilité de refuser l'accès ; la collectivité de santé devra être en mesure de démontrer que cette information au patient a bien eu lieu. La CNPD rappelle dans ce contexte sa recommandation déjà formulée en 2010 que le recours à une « carte de santé » de type « carte vitale française » ou « elektronische Gesundheitskarte » allemande faciliterait ce procédé, de même qu'elle faciliterait l'utilisation d'autres procédés / fonctionnalités dans le cadre du système du DSP (tel que par exemple le recours à un identifiant de connexion peu pratique ou convivial).

La CNPD s'interroge en outre si un patient ne s'oppose pas lors de son admission dans un établissement hospitalier à l'accès à son DSP, est-ce que par défaut tous ceux qui travaillent dans cet établissement auront accès à son DSP ?

A ce titre, le commentaire des articles y répond en précisant qu'en *« cas de séjour dans un établissement, seuls les professionnels de santé intervenant dans la prise en charge du titulaire peuvent accéder à son dossier de soins partagé et* ***non l'ensemble des membres du personnel de cet établissement.*** *»* La CNPD estime cependant que cette précision doit figurer au texte du projet sous avis.

Le commentaire des articles précise dans ce contexte qu'il *« appartient aux collectivités de santé de mettre en place les mesures adéquates en vue d'assurer le respect de cette matrice. »* Pour vérifier la conformité de ces mesures, ainsi que pour permettre aux titulaires des DSP d'avoir un droit de regard sur qui a accédé leur DSP, la CNPD estime

nécessaire que le texte prévoit l'obligation pour les collectivités de santé de mettre en place des systèmes de traçage des accès qui sont nominatifs et individuels. Ainsi, elle recommande aux auteurs d'ajouter à la fin du paragraphe (1) de l'article 9 du projet les mots suivants : *« indépendamment du fait si cette personne est un professionnel de santé individuel ou fait partie d'une collectivité de santé ».*

Enfin, la Commission nationale se demande comment l'« accord » du titulaire qui permet à l'introducteur d'une donnée de limiter son accès en vertu de l'article 8 paragraphe (5) du projet se manifestera concrètement. Est-ce qu'il s'agit d'un consentement écrit du titulaire, acté dans le DSP, ou d'un simple consentement oral ? L'article 7 du RGPD prévoit dans ce contexte que si un traitement repose sur le consentement de la personne concernée, le responsable du traitement doit être en *« mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant. »* En application de cette disposition et sauf modification ultérieure du texte concernant une éventuelle responsabilité conjointe comme préconisée par la CNPD, l'Agence eSanté devrait être en mesure de prouver que le titulaire a consenti à ce que l'introducteur d'une donnée peut limiter son accès tel que prévu audit article 8, paragraphe (5) du projet.

XVIII. Traçabilité des accès et des actions

L'article 9 du projet ne précise pas pendant combien de temps les données de journalisation seront conservées à partir de leur enregistrement. Ce n'est qu'en lisant le commentaire des articles qu'on comprend que la durée de conservation des traces est la même que celle des données du DSP. Or, la CNPD estime nécessaire de préciser la durée de conservation des données de journalisation dans le corps du texte du projet sous examen.

Le paragraphe (2) de l'article en cause prévoit que le titulaire, ses représentants légaux et le médecin référent peuvent consulter l'ensemble des traces des accès et des actions relatives aux données du DSP, hormis celles concernant les données qui leur ont été rendues inaccessibles conformément aux dispositions du présent règlement. En ce qui concerne une limitation des droits des personnes concernées, comme notamment le droit d'accès, l'article 23 paragraphe (1) du RGPD dispose que le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter, entre autres, la portée du droit d'accès prévu par l'article 15 du RGPD. Une telle limitation doit respecter l'essence des libertés et droits fondamentaux et elle doit constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des dix motifs y prévus. Une mesure législative limitative doit d'ailleurs contenir certaines dispositions spécifiques énumérées à l'article 23 paragraphe (2) du RGDP.

Ainsi, comme l'article 9 paragraphe (2) du projet sous examen limite le droit d'accès des titulaires, représentants légaux et médecins référents, cette limitation doit être prévue par une loi au sens stricte du terme et respecter les exigences susmentionnées prévues à l'article 23 du RGPD.

XIX. Délai de versement des données au dossier de soins partagé

L'article 10 paragraphe (3) prévoit que certaines données utiles et pertinentes doivent être versées au DSP au plus tard *« quinze jours après la fin de la prise en charge par le professionnel de santé qui en est l'auteur […] »* La Commission nationale estime qu'il serait utile de définir la notion de « prise en charge », respectivement « fin de la prise en charge ».

Ensuite, conformément à l'article 8 paragraphe (2) du projet, le professionnel de santé, hormis le médecin référent, ne saura en principe plus accéder au DSP d'un de ses patients au-delà du délai de 15 jours après la prise en charge du titulaire. Or, l'article 10 paragraphe (1) du projet est en contradiction avec l'article 8 paragraphe (2) du projet alors qu'il prévoit que le *« professionnel de santé détenteur d'une donnée qu'il estime utile et pertinente au sens de l'article 60quater, paragraphe 2 du Code de la sécurité sociale, verse celle-ci au dossier de soins partagé dans un délai raisonnable après la prise de connaissance de cette donnée ou après son premier accès au dossier de soins partagé si cette donnée est antérieure à son activation. »*

Est-ce que le professionnel de santé pourra donc accéder au DSP en dehors d'une prise en charge du titulaire, alors qu'en principe il n'aura pas accès d'office au DSP sans l'identifiant de connexion du titulaire ? Pourquoi ne précise-t-on pas qu'après l'écoulement d'un délai de 15 jours suivant son premier accès au DSP, le professionnel de santé devra y verser les données qu'il juge utiles et pertinentes et qui sont antérieures à l'activation du DSP ?

En ce qui concerne la conservation des données au DSP, en dehors de l'hypothèse d'une fermeture active par son titulaire, l'article 10 paragraphe (5) du projet prévoit une durée de conservation de dix ans à compter du versement des données dans le DSP, *« à l'exception des informations relatives à l'expression personnelle du titulaire qui sont conservées jusqu'à ce que le titulaire les modifie ou supprime et de certaines données médicales jugées utiles et pertinentes à vie par le médecin qui sont conservées jusqu'à la fermeture du dossier de soins partagé. »*

Au regard du RGPD, il est nécessaire et primordial de définir une durée de conservation des données au sein du DSP, qui soit proportionnée au regard de la finalité du DSP. Partant, il est nécessaire de définir des critères objectifs permettant de justifier une durée de conservation adéquate, étant entendu que le DSP ne se substitue pas au dossier médical tenu par les professionnels de santé *« pendant dix ans au moins à partir de la date de la fin de la prise en charge. »*[76]

L'exposé des motifs du projet précise d'ailleurs que le DSP « n'a pas vocation à être exhaustif mais exclusivement à regrouper parmi les catégories de données mentionnées à l'article 60quater paragraphe 2 celles qui sont utiles et pertinentes pour la continuité et la coordination des soins du patient. »

[76] Selon l'article 15 paragraphe (4) de la loi du 24 juillet 2014 relative aux droits et obligations du patient.

Si le critère retenu est donc celui de la continuité et de la coordination des soins, la durée de cette coordination est nécessairement variable selon la nature de la pathologie et la prise en charge envisagée par les professionnels de santé. Toutefois, suivant le commentaire des articles, les auteurs du projet ont décidé de fixer, sauf exceptions susmentionnées, une durée de conservation unique pour toutes les catégories de données *« étant donné la diversité de données susceptibles d'être versées au dossier et la variabilité dans le temps de leur caractère utile et pertinent respectif dans le parcours de soins […]. »* Les auteurs ajoutent que *« compte tenu de la finalité d'échange et de partage de données importantes pour une meilleure qualité et sécurité dans le parcours des soins, cette durée est fixée de manière à garantir que tous les patients, y inclus ceux qui consultent moins régulièrement, puissent disposer d'un minimum de données importantes dans leur dossier. »*

Or, comme mentionné sous le point *« IV. Fermeture et suppression du dossier de soins partagé »*, les professionnels de santé et en particulier les médecins, représentés par l'AMMD, considèrent par contre qu'une durée de conservation de dix ans ne correspond pas à la réalité des moyens et de l'utilité de la profession, alors qu'ils estiment qu'un professionnel de santé ne serait pas en mesure de consulter les données sur une telle période. Suivant l'adage « trop d'information tue l'information », elle est d'avis qu'un *« temps de conservation de 5 ans ou au-delà ne fera que saturer le DSP de documents inutiles voire obsolètes rendant ainsi laborieuse la consultation du DSP par les médecins et les autres prestataires de santé. »*[77]

Le Collège médical émet des réserves similaires : il est d'avis qu'il faudrait : *« élaborer une stratégie d'hiérarchisation de la pertinence des données et leur révision régulière, en vue de supprimer ou de transférer en arrière-plan les données non pertinentes »* et que *« la conservation d'anciennes données confirmées ou infirmées par de nouvelles données concernant le même objet n'a aucun intérêt »*.[78] Selon le Collège médical, ces données devraient pouvoir être supprimées pour ne pas encombrer inutilement le DSP.

Les principes de minimisation des données et de la limitation de la conservation, exigent que seules des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités spécifiques soient traitées et conservées pendant une durée n'excédant pas celle nécessaire au regard desdites finalités (article 5 paragraphe (1) lettres c) et e) du RGPD). Considérant que le DSP a comme finalité principale le partage et l'échange de données utiles et pertinentes entre professionnels de santé pour une meilleure qualité de soins, que le DSP n'a pas comme vocation d'être exhaustif, qu'il ne se substitue pas aux dossiers tenus par les professionnels de santé ou les établissements hospitaliers et qu'il n'a certainement pas comme finalité de stockage ou d'archivage, la CNPD estime qu'une durée de conservation de cinq ans à compter du versement des données dans le DSP est suffisante et appropriée au regard des finalités réellement et légalement poursuivies.

Comme déjà indiqué sous le point *« IV. Fermeture et suppression du dossier de soins partagé »*, la CNPD estime nécessaire d'intégrer les dispositions concernant la durée de conservation des données au sein du DSP dans une loi, c'est-à-dire dans l'article 60quater du Code de la sécurité sociale, et non pas dans un acte réglementaire.

[77] Avis de l'AMMD du 11 juillet 2017 au sujet du DSP et la durée de conservation des documents qui y sont attachés.
[78] Avis du Collège médical du 29 novembre 2017 sur le projet de règlement grand-ducal sous examen.

Enfin, le paragraphe (5) de l'article 10 prévoit que certaines données médicales jugées utiles et pertinentes à vie par le médecin sont conservées jusqu'à la fermeture du DSP. Le commentaire des articles énumère à titre d'exemple *« des données relatives à des allergies ou maladies chroniques pouvant avoir des conséquences graves ou à des antécédents chirurgicaux importants comme par exemple des transplantations d'organes. »*

La Commission nationale ne remet pas en cause l'utilité de conserver de telles données de santé fondamentales « à vie » dans le DSP. Néanmoins, elle se demande si chaque professionnel de santé qui a accès au DSP d'un titulaire peut inscrire de telles données dans le DSP et si, le cas échéant, le titulaire du DSP sera au moins alerté lors d'une telle inscription ?

XX. Sécurité de la plateforme électronique nationale

La Commission nationale rappelle qu'en vertu de l'article 32 du RGPD, 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 professionnels de santé qui pourraient utiliser des dispositifs mobiles (tablettes) pour accéder à leur compte et aux DSP de leurs patients.

Selon l'article 11 paragraphe (1) du projet, l'Agence eSanté s'engage à mettre en œuvre un système de management de la sécurité de l'information certifié conforme à la Norme internationale ISO/IEC 27001. Néanmoins, la CNPD suggère de préciser dans le texte du projet de règlement grand-ducal le périmètre minimum sur lequel ladite certification ISO devra se porter. Le périmètre devra porter sur l'intégralité des systèmes, processus et éléments organisationnels impliqués directement ou indirectement sur la plateforme et reflétant bien, le cas échéant, la situation de la responsabilité conjointe.

L'article 11 paragraphe (1) lettre e) du projet envisage la *« mise en place d'audits de sécurité annuels »*. L'article 32 paragraphe (1) du RGPD contient dans ce contexte une liste non exhaustive de mesures techniques et organisationnelles que le responsable du traitement et le sous-traitant doivent mettre en œuvre afin de garantir un niveau de sécurité adapté au risque. Une de ces mesures est précisément la mise en place d'une *« procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement »* (article 32 paragraphe (1) lettre d) du RGPD). Si les auteurs du projet de règlement grand-ducal sous avis entendent viser cette disposition du RGPD, ils devraient en préciser les détails dans le corps du texte. Entre autres, la CNPD estime nécessaire de définir si ces audits seront effectués par des auditeurs indépendants ou par des auditeurs externes à l'Agence eSanté. De même, le projet reste muet sur le

périmètre spécifique de ces audits, alors qu'une approche régulièrement adoptée en la matière se manifeste par un plan d'audit tri-annuel validé par le conseil d'administration pour qu'au bout de 3 ans, toutes les procédures ont été auditées.

Le paragraphe (2) dudit article oblige les prestataires et éditeurs d'un programme informatique connecté à la plateforme nationale à mettre en œuvre des mesures de sécurité appropriées au regard de son type, de sa taille, de ses processus ou de ses activités. Or, la CNPD est d'avis que la taille du prestataire ou éditeur n'est pas à considérer comme un critère pertinent dans ce contexte. En effet, l'article 32 paragraphe (1) du RGPD précise que les mesures techniques et organisationnelles à mettre en place doivent être adaptées à *« l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques […]. »* Le risque peut par exemple être particulièrement élevé si un prestataire a accès à un grand nombre de DSP.

Par ailleurs, même si des précisions quant à la notion d'un « prestataire » se retrouvent dans le commentaire des articles *(« Vu la diversité des prestataires susceptibles de se connecter à la plateforme ou d'utiliser l'une de ses applications, à savoir un établissement hospitalier, une pharmacie, un laboratoire d'analyses médicales et de biologie clinique, une association de médecins ou un cabinet individuel et, pour les données mentionnées à l'article 60quater, paragraphe 2 du Code de la sécurité sociale, un réseau d'aides et de soins, un centre semi-stationnaire, un établissement d'aides et de soins, un établissement à séjour intermittent […] »),* la CNPD recommande aux auteurs d'ajouter une définition dudit terme à l'article 1ier du projet.

En ce qui concerne particulièrement les éditeurs d'un programme informatique connecté à la plateforme nationale, on pourrait interpréter l'article 11 (2) du projet de telle manière que ces derniers pourraient se connecter directement à la plateforme. Or, la CNPD tient à souligner qu'il n'est pas acceptable que des acteurs IT aient eux-mêmes un accès direct au DSP, ceci n'étant absolument pas la pratique en la matière.

Enfin, la Commission nationale se demande à quelles intervalles l'Agence eSanté entend mettre en œuvre les mesures de sensibilisation du personnel telles que prévues à l'article 11 paragraphe (2) lettre e) du projet.

XXI. <u>Modalités techniques de versement des données au dossier de soins partagé et interopérabilité</u>

Selon l'article 12 paragraphe (2) alinéa 4 lettre a) du projet, les tests mentionnés au paragraphe 2, alinéa 3 lettre a) dudit article seront effectués non pas par l'Agence eSanté, mais par un organisme ou une société experte en interopérabilité des systèmes de santé. La CNPD se pose surtout la question qui devra assumer les frais concernant les travaux de cet expert, et surtout qui désignera cet expert et sur base de quels critères les compétences de ce dernier seront vérifiées ?

Le paragraphe (2) de l'article 12 du projet continue en ce sens qu'une attestation de conformité sera délivrée par l'Agence eSanté sur base du résultat des tests réalisés par l'expert susmentionné. Or, sur quels critères l'Agence eSanté va-t-elle baser sa décision et comment va-t-elle se décider concrètement ? Est-ce que des représentants ne faisant pas partie de l'Agence eSanté seront impliqués pour garantir l'indépendance de la décision? La CNPD recommande ainsi aux auteurs d'indiquer dans le projet que l'Agence eSanté doit mettre en place un règlement d'ordre intérieur fixant les procédures de délivrance, de blocage et de retrait des attestations afin de garantir une équité de traitement des attestations pour tous les acteurs.

Enfin, dans l'article 12 paragraphe (2) alinéa 6 du projet il est indiqué que l'attestation des résultats des tests reste valable tant qu'aucune modification ne l'affecterait. Or cette approche ne correspond pas au bonnes pratiques en la matière, car même sans changement dans les systèmes, des nouvelles vulnérabilités dans des applications existantes pourraient tout à fait être découvertes et par la suite potentiellement exploitées. Ainsi la CNPD estime qu'une « procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement » telle que préconisée dans l'article 32 (1) (d) du RGPD devrait être mise en place – et ceci indépendamment si des modifications ont eues lieu.

XXII. Coopération et échanges transfrontaliers

La CNPD constate que le transfert de données de santé par l'Agence eSanté au point de contact « santé en ligne » d'un autre État est subordonné au consentement préalable du titulaire. En prenant en considération que ce transfert comportera certainement des catégories particulières de données à caractère personnel, dont notamment des données de santé, la CNPD tient à relever qu'en vertu de l'article 9 paragraphe (1) lettre a) du RGPD, ce consentement par la personne concernée doit être « explicite ».

Enfin, il est important de mentionner qu'en sus des informations prévues à l'article 13 paragraphe (1) du RGPD, l'Agence doit informer les patients sur l'existence du droit de retirer leur consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci (article 13 paragraphe (2) lettre c) du RGPD).

Ainsi décidé à Esch-sur-Alzette en date du 5 avril 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal pris en exécution de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État

Délibération n° 244/2018 du 12 avril 2018

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 8 juin 2016, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par le Service de renseignement de l'État, règlement à prendre en exécution de la loi ultérieure du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État[79].

Par la suite, la CNPD a rendu son *avis relatif au projet de règlement grand-ducal pris en exécution de la future loi portant réorganisation du Service de Renseignement de l'État et au projet de règlement grand-ducal pris en exécution de la loi du 15 juin 2004 relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité.*[80]

Par courrier du 18 décembre 2018, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet des amendements apportés au projet de règlement grand-ducal susmentionné.

La Commission nationale rappelle aussi qu'un premier *avant-projet de règlement grand-ducal portant création et fixant les modalités de fonctionnement d'un fichier relatif au traitement de données à caractère personnel par le Service de Renseignement de l'État* avait déjà été soumis à la CNPD pour avis en 2013 et a donné lieu à l'avis *de la Commission nationale pour la protection des données relatif à l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'État et à l'avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.*[81]

La Commission nationale passe en revue les amendements qui donnent lieu à observations.

[79] Par un courrier du même 8 juin 2016, Monsieur le Premier Ministre avait également invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité, règlement à prendre en exécution de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

[80] Délibération n° 639/2016 du 13 juillet 2016
https://cnpd.public.lu/fr/decisions-avis/2016/SRE.html

[81] Délibération n° 274/2013 du 28 juin 2013
https://cnpd.public.lu/fr/decisions-avis/2013/sre.html

Amendement 1 concernant l'article 3 initial (article 1er nouveau)

L'article 1er nouveau est intitulé *« Catégories de données à caractère personnel traitées par le Service de renseignement de l'État »* et énumère les différentes catégories de données qui *« peuvent faire l'objet d'un traitement ».*

Pour rappel, l'article 1er paragraphe 1. du premier avant-projet de règlement soumis à la CNPD pour avis en 2013[82] prévoyait plus précisément la création d'une base de données dans les termes qui suivent :
« Le présent règlement grand-ducal a pour objet de créer un fichier relatif au traitement de données à caractère personnel, dénommé « e-RSN » à exploiter par le Service de Renseignement de l'État, et d'en fixer les modalités. »

La version initiale du présent projet de règlement datant de 2016 s'appliquait à une « partie active » et une « partie archives ».

Le projet de règlement dans sa version amendée ne parle plus du tout d'un fichier de données ou d'un traitement de données en particulier, mais de manière générale des traitements de données pouvant être effectués par le Service de renseignement de l'État (SRE).

La formulation choisie semble plus proche de la lettre de l'article 10 paragraphe (1) de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État qui prévoit de manière générale que le traitement de données personnelles auquel procède le SRE fait l'objet d'un règlement grand-ducal.

Cependant, cette formulation très générale peut prêter à confusion si on la met en relation avec la liste des catégories de données du projet de règlement sous avis. En effet, le SRE traite bien d'autres données que celles énumérées à l'article 1er nouveau.

Il s'agit en particulier des données obtenues par les différents moyens et mesures de recherche prévues aux articles 5 à 8 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État. On peut citer à titre d'exemple les enregistrements sonores obtenus par le biais des mesures prévues à l'article 7 paragraphe (1) de la prédite loi du 5 juillet 2016 ou les listings de données de trafic de communications électroniques obtenus par le biais des mesures prévues à l'article 7 paragraphe (2) de la cette loi.

Si le règlement est censé couvrir les données obtenues par les différents moyens et mesures de recherche prévues aux articles 5 à 8 de la loi du 5 juillet 2016, il serait également nécessaire de prévoir des précisions quant aux données traitées dans ce cadre.

L'article 1er nouveau ne contient pas d'informations relatives aux personnes concernées. A fortiori, il ne distingue pas entre différents types de personnes concernées.

[82] avant-projet de règlement grand-ducal sur base de l'article 4 paragraphe (1) de la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'État, similaire à l'article 10 paragraphe (1) de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

A ce sujet, il convient de citer l'article 6 du projet de loi 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, article qui dispose ce qui suit :

« Art. 6. Distinction entre différentes catégories de personnes concernées

Le responsable du traitement établit, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que :

a) les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;

b) les personnes reconnues coupables d'une infraction pénale ;

c) les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale, et

d) les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux points a) et b). »

Il résulte dudit article qu'il doit être distingué, par exemple, entre les données de personnes qui sont susceptibles de commettre une infraction et celles de membres de famille[83], voisins etc. de telles personnes. Il serait indiqué que le texte du projet de règlement grand-ducal reflète cette distinction entre différentes catégories de personnes concernées alors que le SRE tombe dans le champ d'application du projet de loi, qui s'appliquera notamment aux traitements de données *« par le Service de renseignement de l'État dans l'exécution de ses missions prévues à l'article 3 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État »* (article 2 paragraphe (2) lettre a)).

La <u>lettre a) du nouvel article 1</u> prévoit que peuvent être traitées les *« les données à caractère personnel résultant de l'accès aux traitements de données à caractère personnel* […] *prévus à l'article 10, paragraphe 2, de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État »*. Concrètement, il s'agit des données d'une série de bases de données étatiques auxquelles le SRE peut accéder. La Commission nationale se demande s'il ne faudrait pas, à l'instar d'autres lois, préciser quelles sont les données auxquelles le SRE peut accéder. En effet, les données des bases de données étatiques auxquelles les membres des parquets et de l'administration judiciaire ainsi que les membres de la Police grand-ducale ont accès sont déterminées en détail par le règlement grand-ducal modifié du 22 juillet 2008 portant exécution de l'article 48-24 du Code d'instruction criminelle et de l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

La <u>lettre c) du nouvel article 1</u> prévoit que peuvent être traitées les *« données à caractère personnel visées à l'article 6, paragraphe 1er de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, à l'exception de celles relatives à l'appartenance syndicale et à la vie sexuelle »*.

[83] L'exemple de membres de la famille est donné dans le commentaire de l'article 1er nouveau dans le contexte des données de santé.

Les traitement de données visés par ledit article 6 paragraphe 1er sont *« les traitements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions, religieuses ou philosophiques, l'appartenance syndicale, ainsi que les traitements de données relatives à la santé et à la vie sexuelle, y compris le traitement des données génétiques ».*

L'article 6 susmentionné soumet le traitement desdites catégories de données (dites données sensibles) à des conditions beaucoup plus sévères que le traitement d'autres catégories de données.

Cependant la loi modifiée du 2 août 2002 a vocation à être abrogée très prochainement[84].

Cette loi et plus particulièrement son article 6 seront remplacés par les textes suivants :

- *Le règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)* et son article 9 pour ce qui concerne plus précisément les données sensibles.
  Ce règlement constituera en quelque sorte le droit commun de la législation relative à la protection des données, mais il ne s'appliquera pas aux traitements de données opérés par le Service de renseignement dont il est question dans le projet de règlement sous avis.

- 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 portant modification de certaines lois (projet de loi n° 7168). Cette loi s'appliquera notamment aux traitements de données *« par le Service de renseignement de l'État dans l'exécution de ses missions prévues à l'article 3 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État » (article 2 paragraphe (2) lettre a)). L'article 10 du projet de loi régit le traitement de données sensibles, plus précisément « le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ».*

Il serait dès lors plus approprié de se référer à l'article 10 du projet de loi n° 7168 plutôt qu'à l'article 6 de la loi modifiée du 2 août 2002 (le cas échéant avec des dispositions transitoires si le projet de règlement grand-ducal sous avis devait être adopté avant le projet de loi n° 7168).

Par rapport à l'article 6 de la loi modifiée du 2 août 2002, les traitements de données biométriques aux fins d'identifier une personne physique de manière unique s'ajoutent donc. En outre, l'article 10 du projet de loi n° 7168

[84] article 62 du projet de loi portant création de la Commission nationale pour la protection des données et la mise en oeuvre 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'État 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 (projet de loi n° 7184).

mentionne les « données concernant la vie sexuelle ou l'orientation sexuelle » alors que l'article 6 de la loi modifiée du 2 août 2002 mentionnait seulement les « données relatives à la vie sexuelle » tout court.

Puisque la version amendée de l'article 3 devenant l'article 1 exclut désormais expressément les données relatives à l'appartenance syndicale et à la vie sexuelle, peuvent être effectués les traitements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions, religieuses ou philosophiques, ainsi que les traitements de données relatives à la santé, y compris le traitement des données génétiques. Concernant ces données, la CNPD a les remarques suivantes :

- En ce qui concerne les empreintes digitales, la CNPD estime qu'elles ne sont pas à considérer comme données génétiques, contrairement à ce que suggère le commentaire des articles. En revanche, il s'agit *« de données biométriques aux fins d'identifier une personne physique de manière unique »* tels que visés par l'article 10 du projet de loi n° 7168. S'il est nécessaire de traiter les empreintes digitales, le plus clair et le plus respectueux du principe de nécessité serait de les mentionner tout simplement de manière explicite dans la liste des catégories de données pouvant être traitées.

- En ce qui concerne les données de santé, la CNPD souligne que le traitement de celles-ci était expressément exclu dans l'avant-projet de règlement lui soumis pour avis en 2013[85].

- Les données à caractère personnel visées à l'article 6, paragraphe 1er de la loi modifiée du 2 août 2002 comprennent également celles dont le traitement révèle l'origine raciale ou ethnique ou encore les convictions religieuses. À admettre que le traitement de telles données ne peut pas être exclu, il doit en particulier être assuré que ces données ne deviennent pas un critère déterminant pour le déclenchement de mesures de recherche. L'Agence des droits fondamentaux de l'Union européenne (FRA) estime à ce sujet ce qui suit : *« The nature of the conflicts in question and the fact that some of them attract persons of specific ethnic and/or religious backgrounds raises additional fundamental rights considerations. Monitoring persons suspected of criminal activity constitutes a legitimate preventive instrument, but measures that consist of surveillance of a specific group or profiling of potential suspects based on ethnicity or religion alone create the risk of unacceptable discriminatory treatment, both under the ECHR and the EU Charter of Fundamental Rights.»*[86] *Par ailleurs, la Commission européenne contre le racisme et l'intolérance (ECRI) recommande aux gouvernements des États membres d'interdire le profilage racial qu'elle définit comme « l'utilisation par la police, sans justification objective et raisonnable, de motifs tels que la race, la couleur, la langue, la religion, la nationalité ou l'origine nationale ou ethnique dans des activités de contrôle, de surveillance ou d'investigation ».*[87]

[85] Article 5 paragraphe 1. numéro 7. de l'avant-projet de règlement

[86] Safeguarding internal security in compliance with fundamental rights law
FRA contribution
High-level conference on a renewed EU Internal Security Strategy
Brussels, 29 September 2014
http://fra.europa.eu/sites/default/files/fra-2014_conference-contribution-iss.pdf

[87] Recommandation de politique générale n° 11 de l'ECRI : La lutte contre le racisme et la discrimination raciale dans les activités de la police
Adoptée par l'ECRI le 29 juin 2007
https://www.coe.int/t/dghl/monitoring/ecri/activities/gpr/en/recommendation_n11/f-RPG%2011%20-%20A4.pdf
En ce qui concerne le champ d'application de cette recommandation, cf. le point 22. de son exposé des motifs :
« Aux fins de cette Recommandation, le terme « police » désigne les agents qui exercent (ou peuvent exercer selon la loi) le pouvoir d'utiliser la force pour faire assurer le respect du droit et le maintien de l'ordre public dans la société, comprenant normalement la prévention et la détection des infractions. […] Cette définition inclut les services secrets et de renseignement ainsi que la police des frontières. »

La CNPD suggère en ce sens l'insertion d'une mention explicite à ce sujet dans le texte du projet de règlement.

La lettre d) du nouvel article 1 prévoit que peuvent être traitées *« les données collectées sur base de la coopération du Service de renseignement de l'État avec les instances nationales et internationales visées à l'article 9 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ».*

Comme le souligne le Conseil d'État, *« une catégorisation des données ne saurait se faire à travers une référence à la manière dont elles ont été obtenues »*[88].

La CNPD estime par ailleurs que le SRE ne devrait pas, dans le cadre des échanges avec d'autres instances nationales et internationales, traiter des données allant au-delà des catégories de données qu'il peut traiter sur un plan purement interne et qui sont énumérées aux lettres a) à c) du présent article 1 nouveau du projet de règlement.

Or, si le SRE, dans le cadre de ces échanges de données ne traite effectivement pas d'autres données que celles énumérées aux lettres a) à c) du présent article 1, alors la lettre d) de l'article 1 n'apporte rien par rapport à l'article 9 de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État et est superfétatoire.

Amendement 2 concernant l'article 4 initial (article 2 nouveau)

L'article 2 paragraphe (1) nouveau relatif à la durée de conservation prévoit en son paragraphe premier que les données traitées par le SRE *« sont maintenues dans les fichiers aussi longtemps qu'elles sont nécessaires à l'accomplissement des missions du SRE ».*

Le deuxième alinéa du même article 2 paragraphe (1) prévoit que, *« par dérogation à l'alinéa précédent, une durée de conservation est applicable aux données à caractère personnel »* énumérées par la suite et fixe différentes durées de conservations y afférentes.

L'article 2 paragraphe (1) alinéa deuxième soulève la question suivante :

Est-ce que les données rentrant dans une des catégories y énumérées sont seulement maintenues dans les fichiers aussi longtemps qu'elles sont nécessaires à l'accomplissement des missions du SRE (alinéa premier), mais, en tout état de cause pas plus longtemps que ne le permettent les délais énumérés à l'alinéa deuxième ? Ou bien sont-elles systématiquement conservées - indépendamment de leur nécessité - jusqu'à l'expiration des délais énumérées au deuxième alinéa ?

[88] Avis du 11 octobre 2016 relatif au projet de règlement sous avis, N° CE : 51.685.

Le respect du principe de nécessité en tant que principe fondamental de la protection des données ne permet que la première des deux interprétations indiquées ci-dessus et le commentaire des articles laisse entendre que telle était aussi l'intention des auteurs du projet de règlement grand-ducal.

Cependant, la CNPD estime que le texte de l'article 2 paragraphe (1) alinéa deuxième devrait être plus clair et précis à ce sujet.

Elle suggère de remplacer la première phrase de l'article 2 paragraphe (1) alinéa deuxième par la phrase suivante : *« En tout état de cause, les délais de conservation suivants ne doivent pas être dépassés : »*

Elle suggère par ailleurs d'intercaler l'article 2 paragraphe (2) entre l'article 2 paragraphe (1) alinéa premier et l'article 2 paragraphe (1) alinéa deuxième, afin d'améliorer la clarté du texte, de sorte que l'article 2 nouveau aurait la teneur suivante :

« Art. 2. – Durée de conservation des données à caractère personnel

(1) Les données à caractère personnel traitées par le Service de renseignement de l'État, désigné ci-après le « SRE », sont maintenues dans les fichiers aussi longtemps qu'elles sont nécessaires à l'accomplissement des missions du SRE.

(2) Une vérification périodique portant sur la nécessité de conserver les données est effectuée conformément à l'article 3.

(3) En tout état de cause, les délais de conservation suivants ne doivent pas être dépassés :

a) pour les données portant sur […]
b) […]
c) […]
d) […] »

Amendement 3 concernant l'introduction d'un nouvel article 3

L'article 3 paragraphe (1) prévoit que *« les agents du SRE en charge d'une opération vérifient au plus tard tous les cinq ans depuis la saisie des données à caractère personnel ou depuis la dernière vérification périodique des données à caractère personnel relatives à la personne. »*

La CNPD accueille favorablement que l'espacement maximal dans le temps entre deux vérifications périodiques a été ramené de 10 ans à 5 ans (soit le délai prévu par l'avant-projet de règlement de 2013).

Elle salue encore l'introduction de contrôles des données obligatoires par le chargé de la protection des données qui sont prévus par le paragraphe (2) de l'article. Elle considère cependant que la notion de sondage est vague. Si les contrôles se font seulement une fois par an et par sondage, on peut se demander quel sera le pourcentage des données effectivement contrôlés et si ce pourcentage sera suffisamment élevé pour contribuer de manière sensible au respect des règles relatives à la protection des données.

En ce qui concerne le terme de « chargé de la protection des données », la CNPD suggère d'adapter d'ores et déjà la terminologie à celle du règlement général sur la protection des données et du projet de loi n° 7168[89] qui utilisent les termes *« délégué à la protection des données ».*

Amendement 8 concernant l'article 9 initial (article 6 nouveau)

L'article 6 nouveau régit les données de journalisation.

Dans ses deux précédents avis, la CNPD avait demandé qu'il soit également prévu que les communications de données à d'autres autorités nationales ou étrangères fassent l'objet d'une journalisation.

Vue la nouvelle version de l'article 6 (évoquant de manière générale tout traitement de données sans mention spécifique notamment de la partie active et de la partie archives), on peut le cas échéant considérer qu'une telle journalisation doit avoir lieu en tout état de cause en vertu dudit article. Néanmoins, la CNPD suggère de prévoir une mention expresse à ce sujet dans le texte du projet de règlement grand-ducal.

Elle estime également nécessaire de prévoir de manière expresse des fichiers de journalisation qui porteront sur les accès du SRE, par un système informatique, aux traitements de données à caractère personnel de différentes administrations en application de l'article 10 paragraphe (2) de la loi du 5 juillet 2016. Rappelons à ce sujet qu'il existe des dispositions similaires prescrivant des fichiers de journalisation pour les accès à différentes bases de données étatiques par les magistrats (article 48-24 paragraphe (4), lettre (b), du Code de procédure pénale) ou par les membres de la Police grand-ducale (article 34-1, 4e alinéa, lettre (b) de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police).

La CNPD n'a pas d'autres observations à formuler en ce qui concerne les amendements soumis pour avis et renvoie pour le surplus à son avis du 13 juillet 2016.

[89] cf. les articles 32 à 34 notamment du projet de loi n° 7168.

Finalement, elle se permet encore de remarquer que son avis du 13 juillet 2016 (délibération n° 639/2016) sur le projet de règlement sous avis portait également sur un projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité. Elle n'a pas connaissance des suites réservées à ce projet de règlement grand-ducal.

Ainsi décidé à Esch-sur-Alzette en date du 12 avril 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif

Avis complémentaire de la Commission nationale pour la protection des données relatif aux amendements gouvernementaux 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'État 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° 279/2018 du 25 avril 2018

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 ».*

Par dépêche du 8 mars 2018, la CNPD a été saisie d'une série d'amendements gouvernementaux au 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'État 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 »).

En date du 28 décembre 2017, la CNPD a adopté un premier avis relatif au projet de loi n° 7184. Elle entend limiter ses observations dans le présent avis complémentaire à l'amendement n° 28 qui insère un nouvel article 71 dans le projet de loi. Ce nouvel article 71 a pour objet de remplacer l'article L. 261-1 du Code du travail par un nouveau texte.

La Commission nationale se pose plusieurs questions fondamentales quant au maintien de cette disposition ainsi qu'à sa conformité à la jurisprudence européenne et au règlement (UE) 2016/679 (ci-après « RGPD »).

1. Le maintien de l'article L. 261-1 du Code du travail, l'application du RGPD et l'abrogation de la loi modifiée du 2 août 2002

Les traitements de données à des fins de surveillance sont actuellement réglés par l'article 10 et 11 de la loi modifiée du 2 août 2002 (ci-après « la loi »), l'article 11 renvoyant à l'article L. 261-1 du CT. Ce dernier vise les traitements à des fins de surveillance sur le lieu de travail opérés par un employeur c'est-à-dire où les personnes concernées par la surveillance sont des salariés ou assimilés, tandis que l'article 10 de la loi vise tous les traitements à des fins de surveillance qui n'ont aucun rapport avec une relation de travail, c'est-à-dire où les personnes concernées sont des tiers non-salariés.

Lorsqu'un employeur effectue un traitement de données à des fins de surveillance, les articles 10 de la loi et L. 261-1 du CT s'appliquent presque toujours cumulativement, alors que dans la très grande majorité de cas, les deux catégories de personnes (salariés et non salariés) sont concernées. (ex : vidéosurveillance dans un supermarché, banque ou administration : les personnes concernées sont toujours des salariés en même temps que des clients, visiteurs etc. ; surveillance des emails : sont concernés les salariés qui communiquent avec des clients, tiers etc….)

Le projet de loi entend cependant abroger l'actuel article 10 de la loi et maintenir sous une forme modifiée l'article L. 261-1 du CT. Il y a donc lieu de constater qu'en fonction des catégories de personnes concernées par un même traitement de données à des fins de surveillance deux régimes législatifs différents s'appliqueront, à savoir :

- les règles du RGPD à l'égard des personnes concernées non-salariées, le RGPD ne contenant cependant pas une disposition spécifique comparable à l'actuel article 10 de la loi ;

- les règles de l'article L. 261-1 du CT tel qu'il est proposé de le modifier à l'égard des salariés.

La CNPD s'interroge donc sur l'applicabilité de ces deux régimes en pratique. En effet, les moyens techniques par lesquels un système de surveillance est opéré ne pourront pas toujours faire une différence entre un salarié et une personne non salariée. Quel régime faudra-t-il appliquer p.ex. aux caméras vidéo dans une zone filmant à la fois des salariés et des personnes non salariées ? Ainsi, une entreprise qui voudrait p.ex. installer un système de vidéosurveillance pour des raisons de sécurité à l'égard de ses salariés et de ses clients, un traitement de données qui est a priori légitime, sous condition que toutes les règles du RGPD soient respectées. Tel qu'il est proposé de modifier l'article L. 261-1 du CT, la délégation du personnel, dans ce cas de figure, pourrait empêcher la réalisation complète de l'installation – pourtant conforme au RGPD qui est un règlement qui prime sur la loi nationale - au motif que les caméras ne pourraient pas être configurées ou programmées de façon à ce qu'elles filment uniquement les clients mais pas les salariés.

Le maintien de l'article L. 261-1 du CT risque ainsi de poser des problèmes juridiques non négligeables dans la plupart des cas de traitements à des fins de surveillance opérés par des employeurs.

2. Non-conformité de l'article L. 261-1 du CT actuellement en vigueur à la jurisprudence européenne

La CNPD estime que l'actuel article L. 261-1 du CT n'est pas conforme à la jurisprudence de la Cour de Justice de l'Union Européenne (CJUE) pour les raisons qui suivent.

L'article L. 261-1 du CT énumère limitativement les cas (au nombre de 5) sur base desquels un employeur peut légitimer un traitement de données à des fins de surveillance. Cette liste limitative déroge aux cas de licéité de l'article 7 de la directive 95/46/CE (transposé en droit national par l'actuel article 5 de la loi) et de l'article 6 du RGPD. Or, dans un arrêt du 24 novembre 2011, la CJUE a jugé que , les *« États membres ne sauraient ni ajouter de nouveaux principes relatifs à la légitimation des traitements de données à caractère personnel à l'article 7 de la directive 95/46/CE ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cet article »*[90]. Notons que les cas énumérés à l'article 7 de la directive 95/46/CE sont identiques à ceux énumérés à l'article 6 paragraphe (1) du RGPD, de sorte que cet arrêt garde toute sa valeur par rapport à l'article 6 du RGPD.

Au regard de cette jurisprudence, la CNPD vient à la conclusion qu'en prévoyant cinq cas de légitimation spécifiques à l'article L. 261-1 du CT pour des traitements à des fins de surveillance, le législateur a ajouté des principes relatifs à la légitimation et a prévu des exigences supplémentaires qui modifient la portée de l'un des six principes prévus à l'article 6 du RGPD et plus particulièrement celui de l'article 6 paragraphe 1 lettre f) qui dispose que *« Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : (…..) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel (…..). »*, de sorte que l'actuel article L. 261-1 du CT n'est pas conforme à la jurisprudence européenne.

En prévoyant une liste limitative de finalités légitimes, le législateur a dès lors exclu qu'un employeur puisse mettre en œuvre un traitement de données à des fins de surveillance pour d'autres finalités et a ainsi prévu des exigences supplémentaires qui modifient la portée du principe ci-avant mentionné.

Le principe de l'article 6 paragraphe 1 lettre f) commande qu'on mette en balance les intérêts respectifs du responsable du traitement de données et de la personne concernée avant de procéder à un traitement de données. Lorsqu'après cet exercice de mise en balance, il s'avère que les droits et libertés des personnes concernées prévalent, le traitement de données seraient à considérer comme disproportionné et ainsi illégal. Or, comme c'est

[90] Arrêt ASNEF du 24 novembre 2011, C-468/10 et C-469-10.

une question d'équilibre, le responsable du traitement peut ajuster et adopter des mesures pour atténuer les risques pour les droits et libertés des personnes concernées.

L'actuel article L. 261-1 du CT enlève donc à l'employeur la possibilité de légitimer un traitement à des fins de surveillance sur le lieu de travail sur base de l'article 5 paragraphe (1) lettre d) de la loi (transposant l'article 7 lettre f) de la directive 95/46/CE), respectivement de l'article 6 paragraphe 1 lettre f) du RGPD à partir du 25 mai 2018, alors que seules les cinq cas de figure de l'article L. 261-1 du CT peuvent légitimer un tel traitement de données.

En conclusion, le droit du travail luxembourgeois, en ce qu'il modifie la portée de l'un des principes de l'article 6 du RGPD et qu'il interdit en quelque sorte à l'employeur de recourir à cette condition de licéité d'une norme pourtant supérieure, n'est ni conforme à la jurisprudence européenne, ni au RGPD, de sorte que l'article L. 261-1 du CT ne peut pas être maintenu dans sa version actuellement en vigueur.

3. Conformité de la proposition de modification de l'article L. 261-1 du CT (article 71 du projet de loi) à la jurisprudence européenne et au RGPD ?

La CNPD accueille donc favorablement que les auteurs du projet de loi, tel qu'amendé, proposent à l'article 71 du texte coordonné du projet de loi de modifier l'actuel article L. 261-1 du CT pour le rendre conforme à la jurisprudence européenne. Elle salue en particulier que cet article ne limite plus les cas sur lesquels un employeur peut se baser pour légitimer un traitement de données à des fins de surveillance et que les dispositions de l'article 6 du RGPD s'appliqueront à ce type de traitement de données.

Ceci dit, il y a encore lieu d'examiner si les autres dispositions de l'article 71 du projet de loi amendé sont conformes au RGPD.

Une des nouveautés prévues par la législation européenne est l'introduction à l'article 5 paragraphe 2 du RGPD du principe de responsabilisation (« accountability ») à l'égard du responsable de traitement. Ceci constitue un changement de paradigme dans la mesure où le législateur a décidé de passer d'un système de contrôle a priori vers un système de contrôle a posteriori par les autorités de contrôles européennes. Ceci signifie que les responsables de traitement n'ont plus besoin de déclarer préalablement à la CNPD leurs traitements de données (système des notifications/autorisations préalables), mais qu'ils doivent mettre en place, en termes de gouvernance interne, toute une série de mesures obligatoires, qui en outre doivent être documentées, pour démontrer leur conformité à la réglementation et que la CNPD est amenée à contrôler.

Parmi ces mesures que le responsable du traitement doit mettre en place, figurent notamment :

- la tenue d'un registre des activités contenant les détails relatifs à tous les traitements de données (remplaçant le système des notification/autorisation) ;

- la désignation, le cas échéant, d'un délégué à la protection des données ;

- la mise en œuvre de mesures de sécurité techniques et organisationnelles ;

- la réalisation d'analyses d'impact relative à la protection des données (AIPD/DPIA), lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, ceci en l'occurrence dans la plus grande majorité des cas de traitements de données à des fins de surveillance ;

- etc.

L'esprit du RGPD et le système de contrôle de l'application du RGPD tel que conçu et voulu par le législateur européen peut se résumer comme suit : les responsables de traitement doivent évaluer et documenter en interne la mise en place de toute une série de mesures obligatoires pour être en mesure de démontrer leur conformité ; la CNPD, de sa propre initiative, sur base de réclamations qu'elle reçoit ou sur base de la procédure de coopération européenne, effectue des contrôles et sanctionne en cas de violation des dispositions du RGPD.

Or, la CNPD est à se demander comment l'article L. 261-1 du CT modifié par le projet de loi s'articule avec le système mis en place par le RGPD et s'il est compatible avec le texte européen.

En effet, si les auteurs du projet de texte entendent d'un côté abroger le système des autorisations préalables pour les traitements à des fins de surveillance, ils réintroduisent de l'autre côté une procédure d'avis préalable.

Il est vrai que l'article 88 du RGPD permet aux États membres de « *prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail.*

Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail ».

La CNPD se demande cependant dans quelle mesure l'article L. 261-1 du CT en projet est censé réellement préciser des règles spécifiques au sens de l'article 88 précité, alors que la procédure d'avis préalable risque de se trouver en conflit avec, voire de tenir en échec les articles 35 et 36 du RGPD.

Quel régime faudra-t-il appliquer à un traitement de données qui est soumis à une analyse d'impact (art. 35 RGPD) et suivant laquelle une consultation de la CNPD s'avère nécessaire en vertu de l'article 36 du RGPD ? Par ailleurs, le RGPD accorde à l'autorité de contrôle un délai de 8 semaines (susceptible d'être prolongé de 6 semaines), pour répondre au responsable du traitement de données par un avis écrit dans le cadre de la procédure de consultation préalable (art. 36.2 RGPD). Le texte de l'article L. 261-1 du CT en projet n'accorde à la CNPD qu'un délai d'un mois.

Comme le soulève aussi le Conseil d'État dans son avis du 30 mars 2018, quelle est la valeur juridique de l'avis visé à l'article L. 261-1 du CT ? *« Le Conseil d'État s'interroge sur le choix d'investir de cette mission la CNPD. Techniquement, la CNPD ne rend qu'un avis. Cet avis la lie pourtant et le Conseil d'État voit mal comment elle pourra, à la suite d'une réclamation ultérieure de la part d'un membre du personnel, adopter une décision contraire à la position prise lors de l'avis. Investir la CNPD d'une compétence d'avis préalable, qui équivaut en réalité à une autorisation, et d'un pouvoir décisionnel ultérieur quant à la légalité du traitement, même s'il est de nature à protéger les droits des intéressés, conduit à une certaine confusion des rôles dans le chef de l'autorité de contrôle appelée à intervenir avant la mise en place du traitement et à le contrôler par après. Dans ce cadre, le Conseil d'État s'interroge encore sur la nature de l'acte adopté par la CNPD. Le terme « prononcer » utilisé dans le texte signifie, aux yeux du Conseil d'État, que l'autorité de contrôle adopte une décision contraignante. En toute logique, un recours devrait être ouvert devant le tribunal administratif en application de l'article 59 du projet de loi sous examen. »*

Toutes ces questions ouvertes ne sont pas précisées par les règles du texte en projet comme l'exige pourtant l'article 88 du RGPD et sont donc sources d'une insécurité juridique importante.

Pour les raisons qui précèdent, la CNPD recommande aux auteurs du projet de loi d'abroger l'article L. 261-1 du CT. En effet, la CNPD considère que le RGPD constitue un référentiel solide et cohérent qui prévoit un nombre important et suffisant de garanties pour protéger les personnes concernées, dont notamment les salariés, et ceci en l'occurrence par rapport à un traitement à des fins de surveillance sur le lieu de travail. Sans vouloir les énumérer en détail, citons le droit de toute personne (que ce soit un salarié individuel ou une délégation du personnel) d'introduire une réclamation auprès de la CNPD en vertu de l'article 77 du RGPD ou encore l'article 35 du RGPD

qui prévoit que pour les traitements qui sont susceptibles d'engendrer un risque pour les personnes concernées, en l'occurrence les salariés, une analyse d'impact relative à la protection des données devra être réalisée – et que sur base de l'article 35.9 l'entreprise devra, le cas échéant, demander l'avis des personnes concernées ou de leurs représentants dans cette démarche. Enfin, le RGPD confère également suffisamment de moyens et de pouvoirs à la CNPD pour sanctionner efficacement et de manière dissuasive les responsables de traitement qui effectuent des traitements de données en violation de la législation.

Si le législateur entend maintenir l'article L.261-1 du CT tel que proposé à l'article 71 du projet de loi, la CNPD estime nécessaire de l'adapter et de le préciser, au regard des observations formulées dans le présent avis, afin de le rendre conforme tant aux exigences de la jurisprudence de la CJUE que du RGPD.

Ainsi décidé à Esch-sur-Alzette en date du 25 avril 2018.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann
Présidente	Membre effectif	Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7248 relatif au financement des travaux d'extension et de perfectionnement du Réseau national intégré de radiocommunication pour les services de sécurité et de secours luxembourgeois et portant modification de la loi du 20 mai 2014 relative au financement du Réseau national intégré de radiocommunication pour les services de sécurité et de secours luxembourgeois

Délibération n° 283/2018 du 27 avril 2018

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

Par courrier du 20 février 2018, Monsieur le Premier ministre a invité la Commission nationale à se prononcer au sujet du projet de loi n° 7248 relatif au financement des travaux d'extension et de perfectionnement du Réseau national intégré de radiocommunication pour les services de sécurité et de secours luxembourgeois et portant modification de la loi du 20 mai 2014 relative au financement du Réseau national intégré de radiocommunication pour les services de sécurité et de secours luxembourgeois (ci-après : « projet de loi »).

Suivant l'exposé des motifs, le projet de loi vise d'une part, à renforcer les moyens financiers afin d'*« accueillir de nouveaux utilisateurs et de perfectionner le fonctionnement du réseau »* et d'autre part, *« à conférer un fondement légal au traitement des données à caractère personnel concernant les agents publics des autorités, administrations et organismes publics découlant de l'utilisation des équipements et services de communication RENITA »*.

L'exposé des motifs précise, en son point 3 relatif à l'évolution du réseau, qu' *« aujourd'hui, plus de 9.000 agents issus de la Police grand-ducale, de l'Administration des Douanes et Accises, de l'Administration des Ponts et Chaussées, de l'Administration des services de Secours et des services d'Incendie communaux, du Centre des Communications du Gouvernement, de l'Armée luxembourgeoise, du Haut-Commissariat à la Protection nationale et du Service de renseignement de l'État »* font partie des utilisateurs du réseau et que *« sous peu, les agents du Service de la Navigation, du Centre de Rétention et de l'Administration pénitentiaires feront aussi partie des utilisateurs »* de ce réseau. Au regard du nombre élevé d'agents concernés et du risque d'atteinte au respect de la vie privée des agents sur leur lieu de travail, la Commission nationale accueille favorablement que le gouvernement entend fonder le traitement des données personnelles traitées via le réseau RENITA par le droit national.

Il importe de prévoir un fondement légal alors que le traitement des données personnelles dans le cadre du réseau RENITA est à considérer comme un traitement de données à des fins de surveillance au sens des articles 10 de la loi modifiée du 2 août 2002 et de l'article 261-1 du Code du travail. En effet, si le traitement de données pourrait encore être légitimé à l'égard des agents publics (salariés), dans une mesure limitée, sur base de l'article L-261-1 du Code du travail, il en va autrement pour ce qui est de la légitimation de la surveillance sur base de l'article 10 de la loi modifiée du 2 août 2002 à l'égard des agents non-salariés, à savoir les sapeurs-pompiers et secouristes volontaires. Seul le consentement pourrait entrer en ligne de compte, mais un tel consentement ne pourrait pas être considéré comme libre au regard des circonstances et du contexte du traitement de données.

En effet, la Commission nationale se réfère à l'arrêt de la Cour constitutionnelle du 29 novembre 2013, selon lequel *« l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements »*[91] et aux avis du Conseil d'État qui rappellent régulièrement que *« dans les matières réservées à la loi formelle, l'exercice du pouvoir réglementaire par le Grand-Duc est subordonné à l'existence d'une disposition législative spécifiant les fins, les conditions et les modalités dans lesquelles un règlement grand-ducal peut être pris »*[92].

A l'aube de l'entrée en application du règlement (UE) 2016/679 général sur la protection des données (ci-après « RGPD »), la légalité de toute nouvelle proposition de législation doit également être examinée à l'égard de ce règlement. En effet, à partir du 25 mai 2018, un nouveau régime de protection des données personnelles s'appliquera dans l'Union européenne aux termes duquel les responsables de traitements seront responsabilisés et devront eux-mêmes garantir leur conformité aux dispositions du RGPD.

Or, l'article 6 paragraphe 3 du RGPD exige que le fondement d'un traitement qui comme en l'espèce tombe sous le champ de l'article 6 paragraphe 1, lettre c), à savoir *« le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »* et lettre e), à savoir *« le traitement est nécessaire 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 »* soit défini par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt publique ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement.

Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application du RGPD, entre autres : les conditions générales régissant la licéité du traitement par le responsable de 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

[91] Cour constitutionnelle, arrêt 108/13 du 29 novembre 2013 (Mém. A n° 217 du 13 décembre 2013, p.3886).
[92] Avis du Conseil d'État du 9 décembre 2014 à l'égard du projet de loi 6588 portant organisation du secteur des services de taxis et modification du code de la consommation, p.11 (article 5). Voir aussi p.19 (article 20).

durées de conservation ; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal,…

Dans le cadre du présent avis, la Commission nationale se limitera à formuler quelques observations relatives à l'article 3 du projet de loi qui insère un nouvel article 5 à la loi du 20 mai 2014 précitée.

1. <u>Quant aux responsables du traitement</u>

Le paragraphe 5 du nouvel article 5 dispose que *« chacune des autorités et administrations est responsable du traitement des données à caractère personnel relatif à l'utilisation du réseau par ses propres agents, conjointement avec le service chargé de la gestion et de la coordination de l'exploitation du réseau au sein du ministère ayant dans ses attributions le réseau national intégré de radiocommunication »*. Toutefois, l'article 5 utilise tantôt la terminologie d' *« autorités, administrations et services publics* (début de l'article 5), tantôt d'*administrations ou organismes publics »* (§ 4) et pour finir d'« autorités et administrations » (§5), de sorte qu'il est finalement peu aisé de savoir qui peut être responsables du traitement dans le cadre de l'utilisation du réseau RENITA. La Commission nationale recommande dès lors d'utiliser une terminologie identique dans l'ensemble de l'article 5.

De plus, il ressort de l'article 5 que les auteurs n'ont pas énuméré les administrations, autorités et organismes publics concernés par le traitement des données personnelles utilisant le réseau RENITA. La Commission nationale s'interroge dès lors sur le fait de savoir si cette absence d'énumération provient du fait que d'autres *« utilisateurs »* seraient susceptibles de se rajouter *« a posteriori »*. Si tel n'est pas le cas, la Commission nationale suggère de lister, dans le texte même de l'article 5, l'ensemble des autorités, administrations et organismes publics qui seront à considérer comme responsables du traitement tel qu'indiqué dans le commentaire de l'article.

2. <u>Quant aux finalités du traitement</u>

Il ressort de la lecture du nouvel article 5 du projet de loi que les finalités sont les suivantes :

- Coordination des opérations ;
- Optimisation des opérations ;
- Préservation de la sécurité et de l'intérêt vital de leurs agents ;
- Protection de, et de secours à, la population ;
- Analyser le déroulement des opérations et examiner d'éventuels incidents ;
- Améliorer des plans et méthodes d'intervention.

La Commission nationale considère ces finalités comme explicites et précises. Elle s'interroge toutefois sur la nécessité de prévoir comme finalité l' *<u>« intérêt vital »</u>*.

Elle estime que cette inclusion est susceptible de créer une confusion entre la notion d'intérêt vital et la notion de sécurité de l'intégrité physique. En effet, la notion d'intérêt vital est reprise comme condition de licéité d'un traitement à l'article 6, paragraphe 1er, lettre (d) du RGPD est applicable dans des situations très particulières et rares tel que, comme mentionné au considérant 46 du RGPD, *« lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaires, notamment les situations de catastrophes naturelles et d'origine humaine »*. Un traitement sur ce fondement ne devrait avoir lieu que lorsque le traitement ne peut manifestement pas être fondé sur une autre base juridique ce qui n'est pas le cas ici, alors que la sécurité de l'intégrité physique des agents est prévue comme étant l'une des finalités de l'utilisation du réseau RENITA.

Par conséquent, afin d'éviter toute confusion avec la notion d' *« intérêt vital »* reprise à l'article 6 du RGPD, la Commission nationale est d'avis qu'il suffit de mentionner comme finalité « la préservation de la sécurité des agents » ce qui englobe, entre autres, la protection de l'intégrité physique des agents.

De plus, comme mentionné auparavant, le présent projet de loi a pour vocation de fonder le traitement des données personnelles traitées via le réseau RENITA par le droit national et ce, conformément à l'article 6.3 du règlement (UE) 2016/679 général sur la protection des données (ci-après « RGPD ») c'est-à-dire sur base des conditions de licéité reprise à l'article 6 paragraphe 1, lettre c), à savoir *« le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »* et lettre e), à savoir *« le traitement est nécessaire 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 »*.

3. Quant aux modalités d'accès aux données à caractère personnel

Les paragraphes (1) à (3) du nouvel article 5 précisent les différentes catégories de données.

Le commentaire des articles précise plus en détail que *« les données traitées sont relatives à l'identité des agents utilisateurs des équipements de communication (portables ou embarqués dans les véhicules), au statut des terminaux et à leur géolocalisation pendant le service ou à l'occasion des interventions, à la date et l'heure des communications émises et reçues et dans une mesure limitée au contenu des messages textes et des communications vocales »*.

A ce titre, la Commission nationale se demande ce que recouvrent les termes *« dans une mesure limitée au contenu des messages textes et communications vocales » tel que repris dans le commentaire des articles.*

Pour ce qui est de la terminologie utilisée au paragraphe (1) « localisation » et au paragraphe (2) « géolocalisation », elle suggère d'utiliser une même terminologie dans l'ensemble de l'article sous analyse.

Par ailleurs, la Commission nationale comprend que seules les directions opérationnelles des autorités, administrations et services publics peuvent accéder en temps réel *« aux indications relatives à la localisation et au statut des terminaux et peuvent suivre depuis leurs postes de commandement les communications émises et reçues par leurs agents en opération y compris avec une fonction de réécoute endéans 3 heures ».*

Il ressort du commentaire des articles qu'uniquement les responsables du pilotage et de la surveillance des interventions peuvent procéder à la réécoute endéans 3 heures aux seules fins opérationnelles. Dans la mesure où les auteurs entendent limiter par la loi la réécoute à un type/fonction spécifique d'agents et pour une finalité bien déterminée, la Commission nationale se demande s'il ne serait pas préférable de l'indiquer dans le texte du paragraphe 1er du projet de loi au lieu de le préciser dans les instructions de service.

Les paragraphes (2) et (3) du nouvel article 5 précisent quant à eux les accès *a posteriori* aux données et ce, dans l'objectif d'analyser le déroulement des opérations, d'examiner d'éventuels incidents ainsi qu'afin d'améliorer des plans et méthodes d'intervention. La Commission nationale n'a pas de remarque particulière concernant les présents paragraphes mais elle suggère de remplacer le libellé du paragraphe (3) par *« le contenu des messages et les conversations sont enregistrées et conservées pendant trois mois au maximum ».*

En ce qui concerne le paragraphe (4) du nouvel article 5, la Commission nationale s'interroge sur l'utilisation du terme *« ponctuellement »*. En effet, ce paragraphe dispose que *« les données ne pourront être consultées que ponctuellement sur décision expresse des chefs des administrations ou organismes publics concernées ou de leurs délégués en vue de l'analyse du déroulement des opérations et de l'examen d'éventuels incidents ainsi que des possibilités d'amélioration de plans et méthodes d'intervention ».*

La Commission nationale suggère d'omettre le mot « ponctuellement » car il est peu clair et contribue à semer confusion.

Elle regrette par contre qu'il n'y ait pas dans le corps du texte de critères ou de précision quant aux facteurs déclencheurs sur base desquels les chefs d'administrations, d'organismes publics ou des délégués prennent leur décision expresse de procéder à (i) une analyse du déroulement des opérations, (ii) l'examen d'incidents ou (iii) l'amélioration des plans et méthodes d'intervention. Conformément au deuxième alinéa du paragraphe (5) de l'article 5 de telles précisions devront être prévues dans les instructions de service internes.

Aux alinéas 2 et 3 du paragraphe (5) du nouvel article 5 du projet de loi, il est en effet précisé que *« les modalités limitatives d'accès aux données enregistrées feront l'objet d'instructions de service internes qui préciseront les mesures techniques et d'organisation à mettre en œuvre en vue de réduire les risques d'atteinte à la sphère privée des agents concernés et de prévenir d'éventuels abus. Ces instructions de service internes feront l'objet d'une consultation préalable de la Commission nationale pour la protection des données ».*

La Commission nationale regrette que dans l'intérêt de la sécurité et de la prévisibilité juridique des personnes dont les données personnelles sont traitées, les modalités d'accès ne soient pas règlementées de façon générale aux termes de la loi. Elle suggère que le texte précise au moins que l'accès aux données ne saurait servir à l'évaluation d'aspects personnels ou du comportement individuel des agents ou à des fins disciplinaires.

La Commission nationale comprend que pour chaque entité utilisatrice du réseau RENITA les modalités d'accès tenant compte de leurs besoins de fonctionnement particuliers doivent obligatoirement faire l'objet d'instructions de service internes qui précisent les mesures techniques et d'organisation à mettre en œuvre en vue de réduire les risques d'atteinte à la sphère privée des agents concernés et de prévenir d'éventuels abus.

Il est vrai que le considérant 41 du RGPD précise que *« lorsque le présent règlement fait référence à une base juridique ou à une mesure législative, cela ne signifie pas nécessairement que l'adoption d'un acte législatif par un parlement est exigée, sans préjudice des obligations prévues en vertu de l'ordre constitutionnel de l'État membre concerné. Cependant, cette base juridique ou cette mesure législative devraient 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 et de la Cour européenne des droits de l'homme »*. A ce titre, la Commission nationale se demande toutefois si l'utilisation d'instructions de service internes suffisent à cette exigence.

En tout état de cause, la Commission nationale salue que le texte prévoit qu'elle devra être demandé en son avis lorsque les instructions de service internes seront mises en place.

4. La durée de conservation des données de géolocalisation GPS, de trafic CDR et d'enregistrement des messages et conversations

En ce qui concerne la durée de conservation des données de géolocalisation et du contenu des messages et des conversations, les auteurs du projet de loi ont prévu une durée de six, respectivement de trois mois.

La Commission nationale estime que ces délais de conservation sont proportionnés au regard des finalités poursuivies.

Ainsi décidé à Esch-sur-Alzette en date du 27 avril 2018

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif

Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif aux amendements parlementaires au projet de loi n° 7184 portant organisation de la Commission nationale pour la protection des données et 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 et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État.

Délibération n° 423/2018 du 8 juin 2018

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 ».*

En date du 28 décembre 2017, la CNPD a adopté un premier avis relatif au projet de loi n° 7184. Un avis complémentaire a été rendu en date du 25 avril 2018.

Suite à une série d'amendements parlementaires, adoptés en date du 14 mai 2018, au projet de loi n° 7184 portant organisation de la Commission nationale pour la protection des données et 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 et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « RGPD »), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, la CNPD se saisit d'office. Elle entend limiter ses observations dans le présent deuxième avis complémentaire aux amendements n° 9, 26, 40 et 41.

Les amendements n° 9 (ancien article 17, nouvel article 14) et n° 26 (ancien article 54)

Le nouvel article 14 prévoit que la CNPD a le *« pouvoir de porter toutes violations des dispositions adoptées en vertu du RGPD »* à la connaissance des autorités judiciaires. La CNPD ne comprend pas le rajout des termes « des dispositions adoptées en vertu du règlement », alors que le paragraphe 5 de l'article 58 du RGPD précise

qu'il doit s'agir de « toute violation du présent règlement ». Le nouvel article 14 limite les pouvoirs de la CNPD par rapport au RGPD, sans pour autant préciser quelle juridiction la CNPD est censée saisir. En l'état, la disposition nationale en question n'a pas de valeur normative, alors qu'elle ne précise pas la procédure judiciaire à suivre par la CNPD pour saisir pro-activement la justice d'une violation du RGPD. Elle avait déjà soulevé cette problématique dans son avis du 28 décembre 2017. Ainsi la CNPD estime que cette question n'est toujours pas suffisamment clarifiée et que la loi en projet n'est pas conforme au RGPD sur ce point.

La Commission nationale regrette par ailleurs que les auteurs des amendements n'ont pas suivi la CNPD dans son avis précité concernant la nécessité de prévoir en droit national une procédure judiciaire telle que l'exige l'arrêt « Schrems » de la CJUE (affaire C-362/14) du 6 octobre 2015. Elle réitère dès lors pour les besoins du présent avis ces observations formulées dans son premier avis à ce sujet.

La CNPD regrette aussi que les auteurs des amendements ont supprimé du projet de loi l'ancien article 54. Elle estime qu'en l'absence de ces précisions il y a un risque qu'elle ne pourra pas faire exécuter judiciairement des mesures correctrices adoptées par elle. Ainsi, par exemple, si la CNPD adopterait une mesure correctrice à l'encontre de l'État ou d'une commune, elle n'aura pas nécessairement de moyens coercitifs suffisants pour faire respecter sa décision, d'autant plus que le régime des sanctions financières et des astreintes ne s'applique pas à l'État ou aux communes.

L'amendement n° 40

L'amendement n° 40 entend remplacer l'article 59 du projet de loi initialement déposé, respectivement l'article 68 du texte coordonné suite aux amendements gouvernementaux du 8 mars 2018. L'amendement propose un nouvel article 63 au Chapitre 3 (du Titre II du projet de loi) intitulé « Traitement de catégories particulières de données à caractère personnel ».

La CNPD voudrait d'emblée relever qu'elle a de sérieux doutes quant à la valeur normative des paragraphes (1), (2) et (3) du nouvel article 63. Malgré les adaptations et modifications textuelles apportées à l'ancien article 68 (article 59 initial), elle ne peut que rappeler et réitérer ses observations formulées dans son premier avis du 28 décembre 2017, à savoir : *« …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 États 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. »*

Rappelons que sauf la lettre j) du paragraphe (2), l'article 9 du RGPD ne fait pas partie des « clauses d'ouverture » du Chapitre IX du RGPD (article 85 à 91), c'est-à-dire des *« Dispositions relatives à des situations particulières de traitement »* qui offrent aux États membres la possibilité de prévoir et de préciser des règles plus spécifiques dans certaines matières par rapport aux règles générales du RGPD.

Les paragraphes (1), (2) et (3) de l'article 9 du RGPD, applicable en droit luxembourgeois depuis le 25 mai 2018, ne nécessitent donc en principe pas de mesures de transposition telles que celles proposées par les paragraphes (1), (2) et (3) du nouvel article 63 dans le présent projet de loi. Seul le paragraphe (4) de l'article 9 du RGPD permet aux États membres de *« 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 »*, auquel la CNPD entend revenir plus loin dans le présent avis.

Ceci dit, la CNPD analysera ci-après les quatre paragraphes du nouvel article 63 du projet de loi.

- Le paragraphe (1) du nouvel article 63 du projet de loi prévoit que le responsable du traitement, lorsqu'il traite des catégories particulières de données pour les finalités prévues à l'article 9 paragraphe 2, lettres b), g) et i) du RGPD, doit mettre en œuvre au moins les cinq mesures de sécurité additionnelles énumérées au points 1° à 5° du paragraphe (1) du nouvel article 63. La CNPD se demande par rapport à quelles autres mesures de sécurité, les mesures de sécurité visées aux point 1° à 5° peuvent être qualifiées d'« additionnelles ». Elle suppose qu'il faut comprendre ces mesures de sécurité comme additionnelles par rapport aux mesures de sécurité prévus et requis par les règles du RGPD. Or, les mesures de sécurité proposées dans le texte peuvent tout au plus être considérées comme des mesures standards et ne peuvent manifestement pas être considérées comme additionnelles, alors que l'article 32 du RGPD exige déjà que le responsable du traitement ou le sous-traitant mette en œuvre des mesures de sécurité techniques et organisationnelles appropriées en tenant en compte du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques. La CNPD s'étonne dès lors que le texte de loi en projet prévoit un niveau de sécurité qui ne semble pas, dans la grande majorité des cas – sans mesures additionnelles spécifiques - satisfaire le niveau exigé par le RGPD dans le cadre de ces traitements de données hautement sensibles. Elle s'interroge donc sérieusement sur la raison d'être et la valeur normative du paragraphe (1) du nouvel article 63 du projet de loi et estime en tout état de cause que cette disposition n'est pas conforme au RGPD, de sorte qu'il y a lieu de la supprimer.

- Le paragraphe (2) du nouvel article 63 du projet de loi prévoit que le responsable du traitement, peut communiquer des catégories particulières de données à des tiers pour les finalités prévues à l'article 9 paragraphe 2, lettres b), g), i) et j) du RGPD après avoir mis en œuvre des mesures de sécurité « additionnelles » énumérées au points 1° et 2° du paragraphe (2) du nouvel article 63. Ces mesures de sécurité additionnelles diffèrent de celles du paragraphe (1).

Tout d'abord, la CNPD s'interroge sur l'utilité de la formulation *« Sous réserve que leur traitement soit en lui-même licite … »*. Pourquoi faut-il préciser que le traitement initial doit être licite, alors que cela devrait être évident ? Elle se demande, par ailleurs, pourquoi le texte fait référence à la lettre j) du paragraphe 2 de l'article 9 du RGPD (traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques), alors que les traitements de catégories particulières de données dans le cadre de ces finalités sont d'ores et déjà réglés par l'article 62 du projet de loi.

La CNPD est cependant particulièrement inquiète du contenu et de la portée de la disposition sous revue. Concernant la portée de la disposition :

La disposition semble rendre légitime de facto la communication de catégories particulières de données à caractère personnel à des tiers pour autant que les finalités du traitement par le tiers sont couvertes par l'article 9 paragraphe 2, points b), g), i) et j) du règlement (UE) 2016/679.

En effet, la communication de données sensibles à des tiers constitue une ingérence grave dans la vie privée des personnes concernées. A cet égard, la jurisprudence constante de la CJUE retient que la base légale doit être suffisamment claire et précise et doit offrir une protection contre d'éventuelles atteintes arbitraires, en définissant elle même la portée de la limitation de l'exercice du droit garanti par la Charte[93]. Pour ce qui est de la notion claire et précise de la base légale, la Cour européenne des droits de l'homme (ci-après « CouEDH ») a énoncé qu'*« on ne peut considérer comme une 'loi' qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé »*[94].

Or, la CNPD est d'avis que la disposition sous avis est très vague et ne respecte pas l'exigence de clarté et de précision de la loi. En effet, le choix des auteurs de l'amendement de l'approche d'ordre fonctionnel au détriment d'une définition d'ordre personnel fait en sorte et comporte le risque que n'importe quel responsable de traitement du secteur public et du secteur privé (administrations, établissements publics, hôpitaux, médecins, laboratoires, asbl du secteur conventionné ,…..) puisse communiquer des données sensibles à n'importe quel tiers, pourvu que la communication des données ait lieu dans le cadre des quatre finalités énumérées, elles-mêmes très générales et vagues et que les mesures de sécurité additionnelles aient été mises en place.

Concernant le contenu de la disposition :

Concernant les soi-disant mesures de sécurité additionnelles, la CNPD tient à constater que la pseudonymisation et le chiffrement des données à caractère personnel font déjà partie des mesures de sécurité explicitement mentionnées dans l'article 32 (1)(a) du RGPD et ne pourront ainsi difficilement être qualifiées de mesures additionnelles en l'occurrence dans le contexte du traitement de catégories particulières de données à caractère personnel. Ceci étant,

[93] Cf. l'arrêt du 17 novembre 2015, *WebMindLicenses Kft. c. Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, C 419/14, ECLI:EU:C:2015:832, point 81.

[94] Cf. les arrêts de la CouEDH, Sunday Times c. Royaume-Uni du 26 avril 1979, série A n° 30, § 61 et CouEDH, *Silver et autres c. Royaume-Uni*, n° 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, série A n° 61, § 86-88.

le point 1° du paragraphe 2 du nouvel article 63 du projet de loi prévoit en premier lieu une anonymisation des données. Or, en réalité et en pratique, dans presque tous les cas l'anonymisation des données est inappropriée, compte tenu de la finalité de la communication des données. Il est en effet difficilement imaginable que le nouveau responsable de traitement puisse effectuer ses traitements sur base de données complètement anonymes. Et si tel était le cas, le RGPD ne s'appliquerait de toute façon pas. Ainsi, le point 1° prévoit en deuxième lieu qu'à défaut d'une anonymisation des données, il y lieu de mettre en place une sécurisation des *« transactions »* telle qu'une pseudonymisation ou un chiffrement des données. La CNPD ne voit pas le lien, ni la logique entre ces deux alternatives, étant donné que la pseudonymisation est une technique de dépersonnalisation de données utilisée pour que les données ne puissent plus être attribuées à une personne sans avoir recours à des informations supplémentaires et que le chiffrement constitue une pure mesure de sécurité informatique en principe appliquée à des données nominatives.

Ensuite, le point 2° reprend une deuxième fois, qu'à défaut d'une anonymisation des données, il y aurait lieu de prévoir une « *procédure de communication des données assurant la conformité du traitement avec le RGPD* ». La CNPD se demande comment le point 1° s'articule avec le point 2° qui chacun prévoit une alternative en l'absence d'une anonymisation des données. Elle a par ailleurs du mal à saisir ce qu'il faut comprendre par la « procédure de communication » visée au point 2°.

Les mesures ainsi proposées par le texte en projet ne peuvent pas être considérées comme des mesures complémentaires ou additionnelles au régime du RGPD et ne peuvent donc pas en elles seules constituer des garanties appropriées et spécifiques pour la sauvegarde des droits et libertés des personnes concernées au sens du RGPD.

Une « communication de données à des tiers » a bien évidemment aussi lieu lors d'un échange ou partage de données, lors d'une interconnexion de fichiers ou encore lors d'un accès direct à des données d'un fichier. Peu importe donc la terminologie utilisée pour décrire une opération de traitement de données qui comporte toujours une communication de données.

La CNPD 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. »*[95]

Le Conseil d'État 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.*

[95] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015.

La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication (…). »[96]

Sur base de ces considérations, la CNPD estime que la licéité des communications de données sensibles à des tiers devrait se retrouver et être couverte par les différentes lois spéciales réglementant les différents domaines et secteurs visés par les finalités dans le texte sous examen (les lois réglementant la santé publique au sens large, loi sur les établissements hospitaliers, loi réglementant certaines professions de santé, lois réglementant la protection sociale, législation en matière de sécurité sociale, lois réglementant le secteur conventionné, …..), c'est-à-dire que les différentes communications, échanges, partages, interconnexions et accès directs devraient trouver leur légitimité au cas par cas dans ces lois qui devraient préciser les entités ou organismes pouvant communiquer ou se faire communiquer des données et pour quelles finalités précises et spécifiques pour autant que ceci ne ressort pas clairement de leurs missions légales.

La CNPD est d'avis que le paragraphe (2) du nouvel article 63 du projet de loi n'a pas sa place dans un texte de loi général comme celui sous examen, alors qu'il ne répond pas aux exigences de précision et de prévisibilité auxquelles doit répondre un texte légal. Eu égard à l'insécurité juridique importante créée, elle estime nécessaire d'omettre cette disposition.

- Le paragraphe (3) du nouvel article 63 du projet de loi entend légitimer de manière générale des échanges de données dans le cadre de l'accomplissement d'une mission légale ou réglementaire pour une finalité cette-fois ci, à savoir celle indiquée à la lettre h) du paragraphe (2) de l'article 9 du RGPD, « sous les conditions visées à l'article 9 paragraphe (3) du RGPD ». La CNPD est à se demander si ce bout de phrase est en l'espèce employé de manière correcte et conforme au RGPD. En effet, à l'endroit de la lettre h) du paragraphe (2) de l'article 9 du RGPD, aux yeux de la CNPD, ce bout de phrase se rapporte uniquement au cas de figure où le « *traitement est nécessaire …… en vertu d'un contrat conclu avec un professionnel de la santé [et soumis aux conditions et garanties visées au paragraphe 3]* » Le paragraphe (3) de l'article 9 du RGPD n'a dès lors vocation à s'appliquer que dans ce cas de figure particulier. Or, les auteurs de l'amendement entendent généraliser l'application de l'article 9 paragraphe 3 du RGPD à tous les échanges de données visés par la disposition sous examen.

  Pour le surplus la CNPD voudrait se référer et reprendre ici toutes ses observations formulées ci-avant relatives au paragraphe (2) du nouvel article 63 du projet de loi. Ainsi, pour les mêmes raisons, elle estime que le paragraphe (3) du nouvel article 63 du projet de loi devrait être supprimé.

- Le paragraphe (4) du nouvel article 63 du projet de loi a pour objet de limiter le traitement de données génétiques conformément à l'article 9 paragraphe 4 du RGPD qui offre cette possibilité aux États membres. Dans son premier avis du 28 décembre 2017, la CNPD s'était souciée que le projet de loi ne contenait pas de dispositions

[96] Voir par exemple : Conseil d'État, 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'État pour études supérieures.

spécifiques relatives aux données génétiques, à l'instar de la loi modifiée du 2 août 2002 sur la protection des données.

La Commission nationale félicite les auteurs de l'amendement d'avoir intégré les dispositions du paragraphe (4) sous examen pour limiter le traitement de données génétiques et ainsi maintenir le niveau de protection en la matière. Les dispositions s'inspirent largement de l'article 6 paragraphe (3) de la loi modifiée du 2 août 2002 sur la protection des données. La CNPD accueille par ailleurs favorablement l'interdiction du traitement de données génétiques en matière de droit du travail et d'assurance.

- Il est un fait que les compagnies d'assurance doivent pouvoir traiter des données de santé pour certains types de contrats d'assurance. Or, au vu de l'approche fonctionnelle choisi par les auteurs de l'amendement n° 40, les compagnies d'assurance ne se retrouvent plus dans la détermination des responsables de traitement pouvant traiter des données de santé. Il s'avère par ailleurs, qu'aucune des conditions de légitimité de l'article 9 paragraphe (2) du RGPD n'est susceptible de légitimer le traitement de données de santé par les compagnies d'assurance. La CNPD est d'avis que le consentement explicite prévu à l'article 9 paragraphe (2) lettre a) du RGPD des personnes concernées ne permet pas de légitimer ce traitement de données, alors qu'il pourrait ne pas être considéré comme libre au sens du RGPD pour certains types d'assurance (p.ex. assurance-vie dans le contexte d'un prêt hypothécaire, assurance solde restant dû, ….). De façon générale, un contrat d'assurance étant un contrat d'adhésion, le consentement n'est en règle générale pas considéré comme approprié pour légitimer le traitement de données de santé dans ce contexte. Dans son avis du 30 mars 2018, le Conseil d'État a également remarqué à l'endroit de l'article 68 que *« se pose encore la question du consentement des personnes concernées dans le cadre de la conclusion d'un contrat d'adhésion »*. La finalité de la « protection sociale » prévue aux lettres b) et h) du paragraphe (2) de l'article 9 du RGPD n'apparaît pas non plus appropriée pour légitimer le traitement de données de santé par les compagnies d'assurance. En effet, les entreprises d'assurances traitent les données de santé non pas à des fins de santé ou de protection sociale, mais bien à des fins commerciales, comme le précise la Conseil d'État dans son avis précité. La protection sociale non autrement définie par le RGPD, n'est pas non plus définie par le droit nationale. Or, la doctrine étrangère analysée par la CNPD constate que les entreprises d'assurance ne font pas partie d'un système de protection sociale nationale lorsque la loi ne le prévoit pas. En effet, les lois françaises et allemandes, par exemple, prévoient expressément que les contrats complémentaires de nature privée d'assurance-maladie sont assimilés à l'assurance-maladie obligatoire et font donc partie du système national de protection sociale. Toujours est-il que les autres types d'assurances indiqués ci-avant ne peuvent pas être considérés comme faisant partie du système de protection sociale. La commission nationale estime donc nécessaire que le projet de loi sous revue prévoit une disposition nationale, conformément à l'article 9 paragraphe (4) du RGPD, pour légitimer le traitement de données de santé en matière d'assurance. Une condition de légitimité appropriée pourrait être celle prévue à l'article 6 paragraphe (1) lettre b) du RGPD. Or, il s'avère que le législateur européen n'a pas prévue cette finalité à l'endroit de l'article 9 du RGPD. La CNPD est d'avis qu'il s'agit là d'un oubli du législateur européen, raison pour laquelle la législation nationale doit remédier à cette carence.

Une telle disposition pourrait voir la teneur suivante : *« Sous réserve des dispositions du règlement (UE) 2016/679, le traitement de données de santé, à l'exception de données génétiques, est licite lorsqu'il est nécessaire à l'exécution d'un contrat d'assurance auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ».*

L'amendement n° 41 (nouvel article 63 bis)

L'amendement n° 41 introduit par l'article 63bis une nouvelle disposition pour limiter les pouvoirs d'accès de la CNPD lui conférés par le RGPD par les lettres e) et f) du paragraphe (1) de l'article 58.

La CNPD estime que la disposition en question ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal, alors que le texte ne précise pas exactement quels lois ou règlements régissant les professions soumises au secret professionnel doivent être respectés. Par ailleurs, pas toutes les lois qui soumettent une profession au secret ne prévoient une procédure spécifique dans le cadre d'enquêtes administratives ou judiciaires. En tout état de cause, la CNPD comprend que dans les cas où la législation ne prévoit pas de règles de procédures spécifiques d'accès aux locaux et aux données, le pouvoir d'enquête de la CNPD ne peut pas être limité, c'est-à-dire que le secret professionnel ne peut lui être opposé. Elle estime qu'en l'état, la disposition nationale en projet ne concilie pas le droit à la protection des données et l'obligation de secret qui s'impose à certaines professions.

Ainsi décidé à Esch-sur-Alzette en date du 8 juin 2018.

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 règlement grand-ducal concernant : 1. la vente par internet au public de médicaments à usage humain; 2. la préparation, la division, le conditionnement ou le reconditionnement des médicaments à usage humain.

Délibération n° 440/2018 du 9 juillet 2018

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

Par courrier en date du 11 décembre 2017, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal concernant : 1. la vente par internet au public de médicaments à usage humain ; 2. la préparation, la division, le conditionnement ou le reconditionnement des médicaments à usage humain (ci-après « le projet de règlement grand-ducal » ou « le projet »).

Le projet de règlement grand-ducal vise à exécuter la loi du 7 juin 2017 modifiant la loi modifiée du 4 août 1975 concernant la fabrication et l'importation des médicaments et 2. la loi modifiée du 25 novembre 1975 concernant la délivrance au public de médicaments.

D'après l'exposé des motifs, ce projet comporte deux volets :

1. les modalités de la mise en œuvre des règles de qualité et de sécurité encadrant les opérations de préparation, de division, de conditionnement ou de reconditionnement des médicaments en officine ou en pharmacie hospitalière ;
2. les modalités de la mise en œuvre de la vente à distance au public de médicaments non soumis à prescription médicale en vue d'adapter la législation en matière de médicaments à usage humain au droit européen .

La CNPD relève 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 ») est applicable dans tous les États membres de l'Union européenne depuis le 25 mai 2018. Ainsi, elle considère qu'il n'y a plus aucun intérêt à analyser le projet de règlement grand-ducal à la lumière de la loi modifiée du 2 août 2002 actuellement toujours en vigueur, mais elle l'avisera uniquement sur base des dispositions du RGPD.

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

Ad article 3 : Sous-traitance

En vertu de l'article 3 paragraphe (1) du projet, la sous-traitance de l'opération en officine ou en pharmacie hospitalière pour le compte d'une autre officine ou pharmacie hospitalière est réservée au pharmacien titulaire, respectivement au pharmacien-gérant. Selon le paragraphe (2) dudit article, même une sous-traitance en dehors d'une officine ou pharmacie hospitalière est possible, si certaines conditions sont respectées.

Dans les deux hypothèses susmentionnées, un contrat de sous-traitance doit être conclu comprenant obligatoirement les mentions prévues au paragraphe (3) de l'article 3 du projet.

En matière de protection des données, le sous-traitant est la *« personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »* (article 4, point 8) du RGPD). Selon l'article 28 du RGPD, le traitement de données à caractère personnel par un sous-traitant doit être régi par un contrat ou un autre acte juridique, liant le sous-traitant à l'égard du responsable du traitement, et prévoyant, entre autres, l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, ainsi que l'obligation pour le sous-traitant de ne traiter les données à caractère personnel que sur instruction documentée du responsable du traitement.

Ainsi, si un éventuel sous-traitant visé à l'article 3 du projet sous examen traite des données à caractère personnel pour le compte d'une autre officine ou pharmacie hospitalière, comme par exemple dans le cadre de l'étiquetage nominatif tel que prévu à l'article 7 paragraphe (2) du projet, la Commission nationale souligne que les dispositions prévues à l'article 28 du RGPD, norme de droit supérieure, s'appliquent également.

Ad article 5 : Les responsabilités et les compétences du personnel

Le commentaire de l'article 5 du projet sous examen prévoit que *« le pharmacien titulaire et le pharmacien-gérant sont responsables pour que les locaux, l'équipement, la coordination des procédures, le personnel et leur formation pratique relative aux opérations de préparation, de division, de conditionnement ou de reconditionnement remplissent les exigences du présent règlement grand-ducal. »*

Selon l'article 24 paragraphe (1) du RGPD et en application du principe de responsabilisation, le responsable du traitement, en l'espèce le pharmacien titulaire respectivement le pharmacien gérant, doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le

traitement est effectué conformément au RGPD. Ledit article prévoit en son paragraphe (2) que lorsque *« cela est proportionné au regard des activités de traitement, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement. »*

Par ailleurs, la CNPD entend souligner qu'en vertu de l'article 32 du RGPD, 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 (incluant les données de santé, telles que des indications sur les médicaments prescrits à une personne désignée) dans la mesure où la divulgation de ces données pourrait causer un préjudice grave aux patients.

Ad article 16 : Compte électronique personnel

L'article 3*octies* alinéas 2 et 3 de la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments prévoit d'un côté que le notifiant[98] est à considérer comme responsable du traitement des données personnelles figurant sur son site internet permettant la vente à distance de médicaments conformément à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et d'autre côté que la *« sous-traitance à un tiers de toute ou partie de l'activité de vente par internet est interdite, à l'exception de la conception et de la maintenance techniques du site internet, qui ne peuvent cependant pas être confiées à une personne produisant ou commercialisant des médicaments ».*

L'article 3decies paragraphe (1) alinéa 1 de ladite loi renvoie à un règlement grand-ducal pour déterminer le contenu obligatoire de l'espace privé qu'un patient doit créer sur le site du notifiant pour commander des médicaments en ligne.

L'alinéa 3 du paragraphe (1) susmentionné prévoit ce qui suit :

« Les données personnelles du patient doivent être gardées pour une durée de deux années depuis la date de la désinscription. Le traitement des données personnelles du patient visées au présent article ne pourra avoir lieu que dans le but de permettre la vente des médicaments par internet, visée par les articles 3bis à 3quaterdecies. Seul le pharmacien a accès aux données personnelles du patient. L'accès de la Direction de la santé lors d'une inspection de la pharmacie du notifiant est limité aux données pseudonymisées du patient. Le patient est informé du traitement de ses données et du droit de désinscription lors de la création du compte. »

Or, la Commission nationale est d'avis que la simple *« indication de la protection des données conformément à loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère*

[98] L'article 1er du projet sous avis définit en son point 7) le notifiant comme *« le pharmacien titulaire exploitant une officine au Luxembourg ayant valablement notifié au ministre ayant la Santé dans ses attributions, ci-après « le ministre », l'activité de la vente par internet au public des médicaments à usage humain avant son début. »*

personnel » (article 16 paragraphe (1) point 10 du projet de règlement grand-ducal) n'est pas suffisant afin de respecter le droit à l'information dont bénéficie toute personne concernée sur base de l'article 13 du RGPD.

Ainsi, la CNPD demande aux auteurs du projet de remplacer le point 10) de l'article 16 paragraphe (1) du projet par une obligation pour le notifiant de fournir les informations prévues à l'article 13 du RGPD à chaque patient qui crée un tel compte électronique personnel sur internet.

Ainsi décidé à Esch-sur-Alzette en date du 9 juillet 2018.

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 n° 6539 relatif à la préservation des entreprises et portant modernisation du droit de la faillite.

Délibération n° 441/2018 du 16 juillet 2018

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

Par courrier en date du 19 mars 2018, Monsieur le Ministre de la Justice a fait parvenir à la CNPD une série d'amendements gouvernementaux au projet de loi n° 6539 relative à la préservation des entreprises et portant modernisation du droit de la faillite (ci-après « les amendements » ou le « projet de loi »).

Pour rappel, la CNPD a rendu, le 20 novembre 2015, un premier avis relatif au projet de loi n° 6539 relatif à la préservation des entreprises et portant modernisation du droit de la faillite[99] dans lequel elle a formulé différentes observations concernant notamment la problématique des données judiciaires, la collecte des données sur les entreprises en difficulté, le droit d'accès, la création d'une base légale pour la transmission de certains jugements au (secrétariat du) Comité de conjoncture, la demande de communication d'informations de la part du (secrétariat du) Comité de conjoncture et la problématique de la liste des protêts.

La CNPD relève 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 ») est applicable dans tous les États membres de l'Union européenne depuis le 25 mai 2018. Ainsi, elle considère qu'il n'y a plus aucun intérêt à analyser le projet de loi à la lumière de la loi modifiée du 2 août 2002 actuellement toujours en vigueur, mais elle l'avisera uniquement sur base des dispositions du RGPD.

La Commission nationale limite ses observations aux amendements n° 6, 7 et 15 qui donnent lieu à observations en rapport avec le respect de la vie privée et avec la protection des données à caractère personnel.

1) Amendement n° 6 concernant l'article 5 initial (article 5 paragraphe (1) nouveau)

a. <u>La détermination du ou des responsable(s) du traitement</u>

[99] Délibération n° 652/2015 du 20 novembre 2015 de la Commission nationale pour la protection des données.

La CNPD note que l'article 5 paragraphe (1) du projet de loi laisse entendre que le secrétariat du Comité de conjoncture est censé agir comme responsable du traitement. Concernant la problématique de la distinction entre le secrétariat du Comité de conjoncture et le Comité de conjoncture lui-même, la Commission nationale renvoie à son avis du 20 novembre 2015. Il en va de même pour la nécessité de la désignation d'un responsable de traitement dans le texte du projet de loi. Les amendements n'ont pas résolu cette problématique mais la CNPD considère toujours que le Comité de conjoncture lui-même agit comme responsable du traitement.

b. Les finalités des traitements de données à caractère personnel et la nature et les catégories de données traitées

La CNPD remarque d'un côté que l'article 5 paragraphe (1) du projet de loi contient désormais une liste des données auxquelles le secrétariat du Comité de conjoncture aura accès aux fins de remplir les missions prévues par le projet de loi. De l'autre côté, les amendements introduisent avec le dernier alinéa de l'article 5 paragraphe (1) un nouveau libellé très vague pour le responsable du traitement. Le fait que le responsable du traitement *« peut joindre au dossier les renseignements et données utiles qui lui sont transmises par le débiteur ou par un créancier (…) »* signifie que la liste des données collectées n'est pas limitative mais peut être élargie librement. Il est indiqué dans le commentaire de l'article 5 paragraphe (1) que les critères ne peuvent pas être définis avec une précision absolue parce que les éléments qui peuvent être pertinents seraient trop nombreux. La Commission nationale est néanmoins d'avis que cette formulation ne répond pas aux exigences de précision et de prévisibilité auxquelles doit répondre un texte légal.

La CNPD rejoint le Conseil d'État qui, dans son avis du 1 décembre 2015, s'est opposé formellement aux dispositions de l'article 5 alinéa 1er initial parce que ces dispositions ont omis *« de préciser comment et d'après quels critères le Comité de conjoncture détermine les débiteurs dont les données seraient collectées »*. Même si les auteurs des amendements ont ajouté à l'article 5 paragraphe (1) alinéa 3 (nouveau) que le secrétariat du Comité de conjoncture estime *« sur base de critères objectifs et vérifiables »* qu'il y a mise en péril de l'entreprise, la CNPD considère que i) cette disposition continue à créer une insécurité juridique et que ii) elle ne permet pas à la CNPD d'examiner si les données traitées sont pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées.

2) Amendement n° 7 concernant l'article 7 paragraphe (2)

La Commission nationale approuve cet amendement utile parce que le droit d'accès et le droit de rectification du débiteur sont déjà abordés par l'article 5 paragraphe (2) nouveau du texte sous examen.

3) Amendement n° 15 concernant l'article 16

La CNPD recommande d'aligner la terminologie sur celle du RGPD et de remplacer les termes « données nominatives » de l'article 16 alinéa 3 (nouveau) par les termes « données à caractère personnel » utilisés par le RGPD.

La CNPD n'a pas d'autres observations à formuler en ce qui concerne les amendements soumis pour avis et renvoie pour le surplus à son avis du 20 novembre 2015.

Ainsi décidé à Esch-sur-Alzette en date du 16 juillet 2018.

La Commission nationale pour la protection des données,

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann
Présidente	Membre effectif	Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7287 portant organisation de la cellule de renseignement financier (CRF) et modifiant : 1. le Code de procédure pénale ; 2. la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ; 3. la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme.

Délibération n° 442/2018 du 16 juillet 2018

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 19 avril 2018, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n° 7287 - projet de loi portant organisation de la cellule de renseignement financier (CRF) et modifiant : 1. le Code de procédure pénale ; 2. la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ; 3. la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme.

La Commission nationale pour la protection des données (CNPD ou Commission nationale) formule les observations ci-après.

<u>Article 74-1 projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire</u>

Au regard de l'article 74-1 alinéa 2 projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ainsi que des articles subséquents, il semble que la CRF devra être considérée - pour les traitements de données prévus par le projet de loi sous avis - comme responsable du traitement au sens de l'article 3 de 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 CNPD note toutefois que loi modifiée du 7 mars 1980 sur l'organisation judiciaire ne définit pas la notion de surveillance administrative alors que l'alinéa premier de l'article 74-1 dispose que la CRF est instituée *« sous la surveillance administrative du procureur général d'État ».*

Article 74-5 projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire

L'article 74-5 projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire dispose en son article premier que *« la CRF donne suite aux demandes motivées d'informations faites par les services et autorités compétents en matière de lutte contre le blanchiment et le financement du terrorisme. »*

La CNPD estime qu'il appartient au législateur d'énumérer les services et autorités compétents pouvant obtenir des informations en vertu de l'article 74-5 projeté. Une telle précision s'impose notamment afin d'assurer le respect de légalité exposé ci-dessous dans le contexte de l'article 74-6 paragraphe (11) projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire.

Article 74-6 paragraphe (2) projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire

L'article 74-6 paragraphe (2) projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire dispose que *« la CRF peut convenir avec une ou plusieurs CRF étrangères d'un mode automatique ou structuré d'échange d'informations. »*

A défaut de précisions, la CNPD comprend cette disposition comme permettant à la CRF de convenir des aspects tels que des formulaires ou des mécanismes électroniques d'échanges à utiliser. Elle n'impliquerait donc pas d'échanges de données allant au-delà de ce qui est déjà prévu par le premier paragraphe de l'article.

Article 74-6 paragraphe (8) projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire

L'article 74-6 paragraphe (8) projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire prévoit ce qui suit :

« Les informations et pièces échangées peuvent uniquement être utilisées par la CRF étrangère aux fins pour lesquelles elles ont été demandées ou fournies. Toute utilisation de ces informations à des fins allant au-delà de celles initialement approuvées est subordonnée à l'autorisation préalable de la CRF.»

La CNPD est sceptique face à une utilisation de données à caractère personnel à des fins autres que celles pour lesquelles elles ont été fournies au départ par la CRF, surtout lorsque les données ont été communiquées à des pays tiers non membres de l'Union européenne. Il convient de rappeler à ce sujet un principe de base de la protection des données qui est le principe de finalité, principe selon lequel des données à caractère personnel ne doivent pas être traitées ultérieurement de manière incompatible avec les finalités pour lesquelles les données ont été collectées.

Pour ce qui est précisément des échanges d'informations à destination d'États tiers qui ne sont pas liés par la directive 2015/849 et d'autres textes européens, il faudrait s'assurer que l'autorité étrangère destinataire des informations ait effectivement connaissance du fait que toute utilisation des informations à des fins allant au-delà de celles initialement approuvées est subordonnée à l'autorisation préalable de la CRF.

Article 74-6 paragraphe (11) projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire

L'article 74-6 paragraphe (11) projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire prévoit que *« la CRF, représentée par son directeur, peut négocier et signer des accords de coopération. »*

Sans mettre en cause la conclusion de tels accords de coopération, la CNPD tient à souligner si de tels accords de coopération peuvent régler certaines modalités, elles ne peuvent pas prévoir d'ingérence au droit au respect de la vie privée allant au-delà de ce que prévoient les lois (ou des traités approuvés par une loi).

Dans ce contexte, la Commission nationale tient à souligner l'importance fondamentale du principe de légalité 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 »*[100]. 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 »*[101]. *« Le degré de précision requis de la « loi » à cet égard dépendra du sujet en question. »*[102]

[100] 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.
[101] 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.
[102] 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.

Au niveau national, la CNPD 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. »*[103]

Afin que le principe légalité sus-énoncé soit respecté, la CNPD se demande s'il ne serait pas indiqué de déterminer dans le texte de loi quels sont les éléments qui pourront être réglés par les accords de coopération.

Article 74-7 projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire

Le nouvel article 74-7 projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire prévoit en son alinéa premier que *« dans le cadre de l'exercice de sa mission, la CRF a un accès direct aux informations contenues au bulletin 1 du casier judiciaire et aux banques de données visées à l'article 48-24 du Code de procédure pénale. »*

Pour la CNPD, il n'est pas clair si cette disposition permet un accès à l'ensemble des données contenues dans les banques de données visées à l'article 48-24 du Code de procédure pénale ou seulement aux données limitativement énumérées par le règlement grand-ducal modifié du 22 juillet 2008 portant exécution de l'article 48-24 du Code d'instruction criminelle et de l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

Le CNPD suggère soit de préciser que les données sont les mêmes que celles auxquelles certains fonctionnaires pourront accéder en vertu de l'article 48-24 du Code de procédure pénale, soit de prévoir qu'un règlement grand-ducal devra préciser les données visées par l'article 74-7 alinéa premier.

Par ailleurs, la CNPD se demande si l'obligation de créer des fichiers de journalisation prévue par l'article 48-24 paragraphe (4), lettre (b), du Code de procédure pénale est applicable aux accès effectués par la CRF en vertu de l'article 74-7 projeté.

L'alinéa 3 du même article 74-7 projeté prévoit que *« la CRF peut accéder, sur simple demande, aux informations administratives et financières nécessaires pour remplir ses missions, détenues par toute autre administration publique. »*

La Commission nationale note que la loi ne définit pas ce que sont des informations administratives et financières.

Est-ce que toute information détenue par une administration dans l'exercice de ces fonctions serait à considérer comme information administrative ?

[103] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015.

Un accès aussi généralisé aux données détenues par les administrations sans autorisation judiciaire préalable semble très problématique au regard des principes de minimisation, de nécessité et de proportionnalité des données.

La CNPD note aussi que le texte ne précise rien quant à la forme de la demande et de la réponse (par écrit, par voie électronique etc.). Si le texte est maintenu tel quel, il faudrait également prévoir une conservation des demandes et réponses pendant une certaine durée, afin de pouvoir retracer a posteriori l'auteur et le motif de la demande. Cela est nécessaire notamment afin de pouvoir identifier des communications de données, le cas échéant, non justifiées.

Article 74-8 projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire

Le nouvel article 74-8 projeté de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire prévoit que *« Le traitement des données personnelles par la CRF est régi par l'article 8 de la loi modifiée du 2 août 2002 relative à la protection des données à l'égard du traitement des données à caractère personnel. »*

Comme le mentionne le commentaire des articles, la loi modifiée du 2 août 2002 devrait être abrogée sous peu, et il faudra tenir compte de l'évolution des projets de loi 7168 et 7184.

En ce qui concerne le fond du renvoi vers l'article 8 précité, la CNPD tient à remarquer que ledit article 8 ne contient pas de règles matérielles en matière de protection des données, mais se borne à renvoyer de manière générale vers les textes applicables en matière de traitements de données judiciaires. Concrètement, un texte de loi spécifique applicable en matière de traitements de données judiciaires (l'article 74-8 projeté sous avis) renvoie vers un article de la loi générale (l'article 8 de la loi modifiée du 2 août 2002) qui à son tour renvoie aux textes de lois spécifiques applicables en matière de traitements de données judiciaires.

Ainsi décidé à Esch-sur-Alzette en date du 16 juillet 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif

Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal pris en exécution de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

Délibération n° 443/2018 du 16 juillet 2018

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 8 juin 2016, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par le Service de renseignement de l'État, règlement à prendre en exécution de la loi ultérieure du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

Par la suite, la CNPD a rendu son *avis relatif au projet de règlement grand-ducal pris en exécution de la future loi portant réorganisation du Service de Renseignement de l'État et au projet de règlement grand-ducal pris en exécution de la loi du 15 juin 2004 relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité.*[104]

Par courrier du 18 décembre 2018, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet des amendements apportés au projet de règlement grand-ducal susmentionné. La CNPD a rendu un avis relatif à ces amendements en date du 12 avril 2018.[105]

Par courrier du 19 juin 2018, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet des amendements apportés audit projet de règlement grand-ducal.

La Commission nationale pour la protection des données formule les observations ci-après.

Amendement 1

L'article 1 paragraphe (2) point 6° nouveau du projet de règlement prévoit que peuvent faire l'objet d'un traitement *« les données en relation avec des évènements, objets, groupements et des personnes physiques ou morales*

[104] Délibération n° 639/2016 du 13 juillet 2016
https://cnpd.public.lu/fr/decisions-avis/2016/SRE.html
[105] Délibération n° 244/2018 du 12 avril 2018
https://cnpd.public.lu/fr/decisions-avis/20171/SRE.html

présentant un intérêt pour l'exercice des missions du SRE obtenus par le biais des mesures prévues à l'article 5, paragraphe 2, de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ».

La CNPD se demande s'il ne serait pas utile d'encadrer encore davantage les données obtenues par le biais des mesures prévues à l'article 5, paragraphe 2, de la loi modifiée du 5 juillet 2016, afin d'exclure tout traitement de données excessif.

On peut aussi par exemple se demander quel sera le traitement réservé à des informations relatives à l'appartenance syndicale ou à la vie sexuelle obtenues par le biais des mesures prévues à l'article 5, paragraphe 2 de la loi modifiée du 5 juillet 2016. Des données de ce type sont exclues par le point 5° de l'article 1 paragraphe (2) du projet de règlement. Mais peuvent-elles faire l'objet d'une conservation en vertu du point 6° du même article 1 paragraphe (2) ?

Amendement 4

L'article 5 nouveau relatif aux fichiers de journalisation évoque désormais le « traitement » au lieu de « l'accès ». La CNPD tient à préciser que l'accès aux données est une forme de traitement de données tout comme l'introduction de nouvelles données, la modification ou la suppression de données.[106] Le « simple » accès aux données est donc a priori couvert par l'article 5.

Néanmoins, la CNPD se demande s'il ne serait pas indiqué de préciser que les dispositions de l'alinéa premier s'appliquent (outre les accès aux données des bases de données propres au SRE) aussi aux accès du SRE, par un système informatique, aux traitements de données à caractère personnel de différentes administrations en application de l'article 10 paragraphe (2) de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

En effet, l'article 10 paragraphe (3) de la loi du 5 juillet 2016 prévoyant des fichiers de journalisation pour lesdits accès ne fixe pas de durée de conservation pour ces fichiers. Par ailleurs, cet article ne précise pas si le motif de la consultation fait l'objet d'un enregistrement.

Ainsi décidé à Esch-sur-Alzette en date du 16 juillet 2018.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann
Présidente	Membre effectif	Membre effectif

[106] L'article 2 paragraphe (1) point 2° du projet de loi n° 7168 tel qu'amendé définit le traitement comme *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».*

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 6961 portant 1. création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2) du Code pénal.

Délibération n° 444/2018 du 16 juillet 2018

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 21 juin 2018, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet du projet de loi n° 6961 portant 1. création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2) du Code pénal.

Pour rappel, par un courrier du 8 juin 2016, Monsieur le Premier Ministre avait invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité, règlement à prendre en exécution de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité. La CNPD avait avisé ledit projet de règlement grand-ducal en date du 13 juillet 2016[107].

Auparavant, en 2013, la CNPD avait déjà rendu un avis relatif à un avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.[108]

Amendement 21

L'article 28 nouveau projeté (remplaçant l'article 22 actuel) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité prévoit que, dans *« le cadre des enquêtes de sécurité ou des enquêtes de sécurité ultérieures, l'Autorité nationale de Sécurité a accès direct, par un système informatique »,* à un certain nombre de bases de données d'administrations publiques énumérées par ledit article.

[107] Délibération n° 639/2016 du 13 juillet 2016
https://cnpd.public.lu/fr/decisions-avis/2016/SRE.html
[108] Délibération n° 274/2013 du 28 juin 2013
https://cnpd.public.lu/fr/decisions-avis/2013/sre.html

La Commission nationale se demande s'il ne faudrait pas, à l'instar d'autres textes légaux, préciser quelles sont les données auxquelles l'ANS peut accéder. En effet, les données des bases de données étatiques auxquelles les membres des parquets et de l'administration judiciaire ainsi que les membres de la Police grand-ducale ont accès sont déterminés en détail par le règlement grand-ducal modifié du 22 juillet 2008 portant exécution de l'article 48-24 du Code d'instruction criminelle et de l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

La CNPD estime également nécessaire de prévoir de manière expresse des fichiers de journalisation qui porteront sur les accès de l'ANS, par un système informatique, aux traitements de données à caractère personnel de différentes administrations en question. Rappelons à ce sujet qu'il existe des dispositions similaires prescrivant des fichiers de journalisation pour les accès à différentes bases de données étatiques par les magistrats (article 48-24 paragraphe (4), lettre (b), du Code de procédure pénale) ou par les membres de la Police grand-ducale (article 34-1, 4e alinéa, lettre (b) de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police)[109].

La version de l'article 22 telle que prévue par la version initiale non amendée du projet de loi sous avis prévoyait d'ailleurs en son paragraphe (5) :

> *« […] l'Autorité nationale de Sécurité met en œuvre les moyens techniques permettant de garantir le caractère retraçable de l'accès.*
>
> *A cette fin, le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que :*
>
> *a) le membre de l'Autorité nationale de Sécurité ne puisse consulter les traitements de données à caractère personnel visés au paragraphe 1er ci-dessus que pour un motif précis en indiquant son identifiant numérique personnel, et*
>
> *b) les informations consultées, la date et l'heure de la consultation puissent être retracées. »*

A cette disposition, la CNPD aurait proposé de rajouter encore que le motif de la consultation doive pouvoir être retracé (alors que dans la version non amendée du projet de loi, il était seulement prévu que les informations consultées, la date et l'heure de la consultation doivent pourvoir être retracées) et elle aurait suggéré de prévoir un délai de conservation de 5 ans pour ces fichiers de journalisation.

Elle ne partage pas la justification donnée dans la motivation de l'amendement selon laquelle la suppression de cette disposition permettrait *« d'éviter un double-emploi avec la loi du jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en*

[109] Article 43 de la future loi sur la Police grand-ducale.

matière de sécurité nationale qui s'applique entièrement au traitement des données recueillies aux fins du présent texte. »

En effet, si 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 prévoit certains principes qui doivent être respectés en matière de traitement de données à caractère personnel, elle ne se substitue nullement aux lois spécifiques traitant des différents traitements à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Enfin, la CNPD note encore que l'article 28 paragraphe (1) dernier alinéa projeté de la loi modifiée du 15 juin 2004 prévoit, en matière d'extraits du casier judiciaire, que *« l'ANS transmet sur base trimestrielle la liste de ses demandes de délivrance et les motifs de ces demandes à l'autorité de contrôle spécifique prévue à l'article 17 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ».* Elle suggère d'adapter cet article au vu du projet de loi n° 7168 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.

Amendement 22

La CNPD constate que l'actuel article 23 de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité (ci-après aussi la loi modifiée du 15 juin 2004), devenant l'article 29 de la même loi suites aux modifications apportés par les amendements sous avis, ne prévoit dorénavant plus que le traitement de données à caractère personnel par l'Autorité nationale de Sécurité (ANS) fasse l'objet d'un règlement grand-ducal. Le projet de règlement grand-ducal avisé par la CNPD en date du 13 juillet 2016 deviendrait donc sans objet.

La CNPD estime que les éléments essentiels des traitements de données à caractère personnel effectués par l'ANS devraient être déterminés par la loi et que certains détails peuvent être réglés par un règlement grand-ducal.

Dans ce contexte, la Commission nationale tient à souligner l'importance fondamentale du principe de légalité 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 »*[110]. 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 »*[111]. *« Le degré de précision requis de la « loi » à cet égard dépendra du sujet en question. »*[112]

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 »*[113].

En l'espèce, la CNPD déplore en particulier qu'aucun texte légal ne fixe de durée de conservation précise pour les données à caractère personnel traitées par l'ANS. En effet, l'article 29 paragraphe (3) projeté la loi modifiée du 15 juin 2004 dispose seulement que *« les données relatives à l'enquête de sécurité sont détruites ou effacées conformément aux dispositions de la loi du jj/mm/aaaa 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 »* sans faire de référence à une disposition précise de cette loi aussi en projet.

La CNPD constate aussi que le projet de loi ne comporte pas de dispositions relatives à des fichiers de journalisation pour ce qui est des accès aux données traitées par l'ANS, alors que les projets de règlement précédemment soumis à la CNPD pour avis comportaient des dispositions à ce sujet.

Par ailleurs, la CNPD note que le texte ne précise pas qui décide quels sont les agents ayant accès aux traitement de données effectuées par l'ANS.

[110] 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.
[111] 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.
[112] 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.
[113] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015.

En ce qui concerne les catégories de données traitées, le texte ne contient pas d'énumération. Cependant, l'article 31 projeté de la loi modifiée du 15 juin 2004 (article 24bis selon la numérotation des articles antérieure aux amendements) déterminera les *« éléments »* à prendre *« en considération »* lors d'une enquête. La CNPD regrette que le texte ne donne aucune précision sur l'origine des données. Il serait préférable que le texte fasse au moins une distinction entre les données que le demandeur d'une habilitation doit fournir lui-même et celles qui sont collectées à partir d'autres fichiers étatiques ou encore par d'autres moyens de recherche.

Ainsi décidé à Esch-sur-Alzette en date du 16 juillet 2018.

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 n° 7269 complétant le Code du travail en portant création d'une activité d'assistance à l'inclusion dans l'emploi pour les salariés handicapés et les salariés en reclassement externe.

Délibération n° 445/2018 du 16 juillet 2018

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

Par courrier en date du 21 mars 2018, Madame la Ministre de la Famille et de l'Intégration a invité la Commission nationale à se prononcer sur le projet de loi n° 7269 complétant le Code du travail en portant création d'une activité d'assistance à l'inclusion dans l'emploi pour les salariés handicapés et les salariés en reclassement externe (ci-après « le projet de loi »).

D'après l'exposé des motifs, ce projet de loi vise *« à faciliter l'intégration, et surtout le maintien dans l'emploi des personnes ayant le statut de salarié handicapée ou étant en reclassement externe, par la création d'une activité appelée « assistance à l'inclusion dans l'emploi » (ci-après « activité d'assistance »). »*

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.

Elle salue le degré de détail avec lequel les auteurs du projet de loi précisent dans l'article L.553-4 nouveau, paragraphe (2) du Code du travail les données à caractère personnel que le formulaire de demande d'assistance à l'inclusion dans l'emploi établi par l'Agence pour le développement de l'emploi (ci- après « l'ADEM ») doit contenir. La Commission nationale peut admettre que les catégories de données traitées sont adéquates, pertinentes et non excessives par rapport aux finalités recherchées. En effet, l'article 6, paragraphe (3) du RGPD précise que le droit de l'État membre auquel le responsable du traitement est soumis 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 ».

Le considérant (41) précise dans ce contexte qu'une base juridique ou une mesure législative *« 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. »*

Par ailleurs, la Commission nationale tient à remarquer que l'article L.553-4 nouveau, paragraphe (2) du Code du travail prévoit des traitements portant sur des catégories particulières de données à caractère personnel (données dites « sensibles »), notamment des données concernant la santé des personnes concernées telles que le type de handicap du salarié, respectivement les incapacités du salarié en reclassement externe. Outre l'hypothèse d'un consentement explicite de la personne (article 9 paragraphe (2) lettre a) du RGPD), plusieurs situations peuvent légitimer un traitement portant sur de telles catégories particulières de données à caractère personnel, en particulier des données de santé. C'est notamment le cas lorsque *« le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un 'État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée »* (article 9 paragraphe (2) lettre g) du RGPD).

Ainsi, la Commission nationale se doit de souligner 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 »*[114]. 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 »*[115]. *« Le degré de précision requis de la « loi » à cet égard dépendra du sujet en question. »*[116]

Le principe de sécurité juridique, qui constitue un des principes généraux du droit de l'Union européenne, exige notamment dans ce contexte « qu'une réglementation entraînant des conséquences défavorables à l'égard de particuliers soit claire et précise et son application prévisible pour les justiciables. »[117]

Ainsi, en prenant en compte les principes susmentionnés de licéité et de sécurité juridique, la CNPD suggère aux auteurs du projet de loi sous avis de préciser dans le corps du texte la durée de conservation des données contenues dans le fichier d'assistance. En effet, l'article 5, paragraphe (1), lettre (e) du RGPD impose au responsable de traitement de veiller à ce que les données qu'il traite ne soient pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Ainsi décidé à Esch-sur-Alzette en date du 16 juillet 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif

[114] 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.

[115] 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.

[116] 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.

[117] Tribunal de l'Union européenne, arrêt du 16 juin 2011, Heineken Nederland BV et Heineken NV c/ Commission, T-240/07, ECLI:EU:T:2011:284, point 383.

Avis de la Commission nationale pour la protection des données à l'égard de l'avant-projet de règlement grand-ducal portant modification 1° de l'arrêté grand-ducal modifié du 23 novembre 1955 portant règlement de la circulation sur toutes les voies publiques, 2° du règlement grand-ducal modifié du 26 janvier 2016 sur le contrôle technique des véhicules routiers et 3° du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers.

Délibération n° 449/2018 du 16 juillet 2018

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 en date du 3 mai 2018, Monsieur le Ministre du Développement durable et des Infrastructures a invité la Commission nationale à se prononcer sur l'avant-projet de règlement grand-ducal portant modification 1° de l'arrêté grand-ducal modifié du 23 novembre 1955 portant règlement de la circulation sur toutes les voies publiques, 2° du règlement grand-ducal modifié du 26 janvier 2016 sur le contrôle technique des véhicules routiers et 3° du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers (ci-après : « l'avant-projet de règlement grand-ducal »).

Suivant l'exposé des motifs, l'avant-projet de règlement grand-ducal vise à *« simplifier les procédures administratives en vue de l'immatriculation des véhicules routiers et de leur contrôle technique en autorisant le recours à la voie électronique pour vérifier la validité des pièces justificatives obligatoires par le biais d'une interface informatique dédiée »*. Pareille vérification est obligatoire pour immatriculer un véhicule (via la Société nationale de la circulation automobile, ci-après « la SNCA ») et pour l'accès au contrôle technique auprès d'un organisme de contrôle technique (actuellement via la Société nationale de contrôle technique, ci-après « la SNCT », ou via la société DEKRA). Les vérifications se font actuellement principalement par contrôle visuel des documents papiers. L'avant-projet de règlement grand-ducal vise également à donner accès aux compagnies d'assurance aux données techniques d'un véhicule particulier qui sont nécessaires pour conclure un contrat d'assurance en responsabilité civile.

La CNPD limite ses observations aux questions traitant des aspects portant sur la protection des données à caractère personnel, soulevées par les articles 2 et 3 de l'avant-projet de règlement grand-ducal, en ce qu'ils octroient à différentes organisations certains accès électroniques à des données à caractère personnel.

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 ») est applicable depuis le 25 mai 2018. Il convient donc d'analyser l'avant-projet de règlement grand-ducal à la lumière du RGPD.

De manière générale, la CNPD comprend l'objectif de simplification des procédures administratives poursuivi par l'avant-projet de règlement grand-ducal. Elle comprend ainsi la nécessité de mettre en place de nouveaux mécanismes de vérification des pièces justificatives obligatoires aux fins d'immatriculer une voiture ou de la présenter au contrôle technique, dès lors qu'une vérification manuelle peut poser certains problèmes en pratique, par exemple en cas de présentation d'une fausse carte verte (difficilement vérifiable par l'organisme de contrôle technique) ou en cas d'oubli, d'altération ou de perte du document. Par ailleurs, la CNPD comprend à la lecture des documents lui soumis par Monsieur le Ministre du Développement durable et des Infrastructures que les auteurs de l'avant-projet de règlement grand-ducal entendent régulariser certaines pratiques d'échanges de données à caractère personnel qui se sont établies, au fil des années, entre certains acteurs du domaine en dehors d'un cadre légal ou réglementaire défini.

Néanmoins, la Commission nationale remarque que les différents accès et échanges de données mis en place par l'avant-projet de règlement grand-ducal pourraient être clarifiés. En effet, à la lecture du texte, il n'est pas toujours clair de savoir quel acteur a accès à quelles données, depuis quelle source et via quel moyen. En outre, la Commission nationale constate que l'avant-projet de règlement grand-ducal et les échanges mutuels de données qu'il met en place entre des acteurs du secteur public (SNCA, SNCT) et du secteur privé (DEKRA, compagnies d'assurance) présentent certains risques d'un point de vue de la protection de la vie privée et des données à caractère personnel qu'il convient d'encadrer plus strictement. Enfin, elle regrette que l'avant-projet de règlement grand-ducal ne contienne pas de dispositions encadrant plus clairement certains des traitements de données à caractère personnel créés. La CNPD tient dès lors à développer ci-après les points qui méritent d'être clarifiés et développés dans l'avant-projet de règlement grand-ducal, afin que les principes fondamentaux auxquels doit satisfaire tout traitement de données à caractère personnel soient respectés.

1) <u>Remarques préliminaires</u>

L'avant-projet de règlement grand-ducal met en place des échanges de données à caractère personnel à plusieurs niveaux. Tout d'abord, l'article 2, point 1° de l'avant-projet de règlement grand-ducal, qui remplace l'article 5 du règlement grand-ducal modifié du 26 janvier 2016 sur le contrôle technique des véhicules routiers, prévoit que *« aux fins de vérifier le respect des conditions prévues à l'alinéa 1er [de l'article 5], l'organisme de contrôle technique est autorisé à accéder par voie électronique aux données nécessaires à travers une interface mise à disposition par le Centre des Technologies de l'Information de l'État, qui transmet l'information demandée de la compagnie d'assurance couvrant le véhicule en question à l'organisme de contrôle technique ».* Un premier accès

à des données est donc créé : celui des organismes de contrôle technique (actuellement, la SNCT et DEKRA) à des données traitées par les compagnies d'assurance, via une interface informatique mise en place par le CTIE.

Ensuite, l'article 3 de l'avant-projet de règlement grand-ducal, qui introduit un nouvel article 12bis dans le règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers, prévoit que *« Aux fins de vérification de l'accomplissement des exigences dont question à l'article 10, la SNCA est autorisée à accéder aux données et à y effectuer des requêtes automatisées en temps réel »* et que *« Les compagnies d'assurance sont autorisées à consulter par voie électronique à travers une interface mise à disposition par le Centre des Technologies de l'Information de l'État les données techniques des véhicules routiers nécessaires à la délivrance de l'attestation d'assurance dont question à l'article 12 ».* Deux autres accès sont ainsi créés : celui de la SNCA à certaines données, dont certains aspects devraient être précisés, d'une part ; et celui des compagnies d'assurances aux « données techniques » via une interface informatique mise en place par le CTIE, dont certains aspects devraient également être précisés, d'autre part.

Sur le principe même de la création d'un accès à la base de données d'acteurs du secteur privé par un acteur du secteur public – et vice-versa –, la CNPD souligne la nécessité de respecter les principes de proportionnalité et de nécessité, selon lesquels tout traitement de données à caractère personnel doit être proportionné aux finalités à atteindre, compte tenu du risque que le traitement fait peser pour la vie privée des personnes concernées.

Il s'agit en effet d'éviter une prolifération des accès d'une administration aux fichiers d'entreprises privées (et vice-versa), si ces accès n'apparaissent pas comme proportionnés et nécessaires par rapport aux intérêts (publics) distincts qu'elles poursuivent.

La Commission nationale comprend que les accès donnés à la SNCA et aux organismes de contrôle technique pourraient permettre d'atteindre la finalité envisagée, à savoir la simplification des procédures administratives en vue de l'immatriculation des véhicules routiers et de leur contrôle technique. L'objectif poursuivi par l'accès donné aux compagnies d'assurance aux données techniques d'un véhicule particulier n'est par contre pas clair à la lecture de l'avant-projet de règlement grand-ducal et devrait dès lors être clarifié.

En tout état de cause, l'objectif poursuivi par les différents accès doit être mis en balance avec le droit pour les personnes concernées à la protection de leur vie privée. Ce dernier élément constitue un droit fondamental consacré notamment par l'article 11 (3) de la Constitution, par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ainsi que par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Il s'agit donc de vérifier si cette balance des intérêts penche en faveur du droit fondamental au respect de la vie privée, qui protège l'intérêt des citoyens, ou en faveur de l'intérêt légitime de l'administration à la simplification de ses procédures, voire aux finalités poursuivies par les compagnies d'assurance (qui devraient être clarifiées), en tenant compte du critère de proportionnalité et de nécessité.

Par ailleurs, étant donné les risques qu'implique la création de tels accès pour la protection de la vie privée et des données à caractère personnel, la Commission nationale tient à 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 »*[118].

Le Conseil d'État 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 (...) »[119].

Dès lors, la Commission nationale se demande si le principe même de la création d'un accès à une base de données d'acteurs du secteur privé par un acteur du secteur public – et vice-versa – ainsi que les finalités (précises) de tels accès, ne devraient pas être prévus dans une loi. Le cas échéant, certains éléments moins essentiels pourraient être intégrés dans le présent avant-projet de règlement grand-ducal.

2) <u>Détermination du rôle des acteurs concernés</u>

Comme indiqué dans les remarques préliminaires ci-dessus, plusieurs opérations de traitements de données à caractère personnel (plus particulièrement des accès) sont créées par les articles 2 et 3 de l'avant-projet de règlement grand-ducal. Ces opérations de traitements impliquent différents acteurs, tels qu'actuellement la SNCA, les organismes de contrôle technique (la SNCT, DEKRA), les compagnies d'assurance et le CTIE.

Suivant le RGPD, les différentes parties impliquées dans un traitement de données à caractère personnel peuvent avoir différentes qualités (par exemple, un acteur peut être qualifié de responsable du traitement, de sous-traitant, de destinataire, etc.) et ces qualités déterminent leurs responsabilités et obligations respectives. C'est le « responsable du traitement » qui se voit attribuer le plus grand nombre de responsabilités. Ainsi, il sera par exemple garant des principes prescrits à l'article 5 du RGPD, il sera responsable des obligations d'information des articles 12 et suivants du RGPD, etc. Le responsable du traitement est *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (…) »*[120]. Il est à noter que deux ou plusieurs responsables du traitement peuvent être « responsables conjoints du traitement » lorsqu'ils déterminent conjointement les finalités et les moyens d'un traitement[121]. Le sous-traitant, quant à lui, est *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme*

[118] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015.
[119] Voir par exemple : Conseil d'État, 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'État pour études supérieures.
[120] Article 4, 7) du RGPD.
[121] Article 26 du RGPD.

qui traite des données à caractère personnel pour le compte du responsable du traitement »[122]. La qualification d'un acteur en tant que responsable du traitement, sous-traitant, destinataire ou tiers a d'importantes implications, principalement en terme d'obligations à respecter. Il est à noter que la qualification d'un acteur est à apprécier en fonction d'un traitement de données à caractère personnel particulier. Ainsi, un acteur peut par exemple être considéré comme responsable du traitement dans le cadre d'un traitement particulier et comme sous-traitant dans le cadre d'un autre traitement.

L'avant-projet de règlement grand-ducal, tel qu'il est actuellement rédigé, ne permet pas de saisir clairement la qualité, et ainsi les responsabilités, des différents acteurs impliqués dans chacun des traitements de données.

Dans le cadre de l'article 4, paragraphe 7 de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques, la Commission nationale comprend par exemple que le Ministre ayant les transports dans ses attributions agit en qualité de responsable du traitement des données à caractère personnel traitées notamment dans le cadre de l'immatriculation des véhicules (le « fichier national des véhicules routiers »). En assurant la gestion de ces données, la SNCA agit, elle, comme sous-traitant dudit Ministre. La Commission nationale doit-elle comprendre que ces acteurs revêtent des qualités similaires dans le cadre du présent avant-projet de règlement grand-ducal ? Le CTIE est-il également à considérer comme un sous-traitant ? Qu'en est-il des assureurs ou encore des organismes de contrôle technique ?

3) <u>Détermination des finalités de traitement</u>

Conformément à l'article 5.1 (b) du RGPD, les données à caractère personnel doivent être *« collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (…) ».*

La Commission nationale salue le fait que la finalité du traitement institué par l'article 2, point 1° de l'avant-projet de règlement grand-ducal, qui modifie l'article 5 du règlement grand-ducal modifié du 26 janvier 2016 sur le contrôle technique des véhicules routiers, soit indiquée. En effet, d'après ledit article, l'accès des organismes de contrôle technique aux données des compagnies d'assurances ne peut se faire qu' *« aux fins de vérifier les conditions prévues à l'alinéa 1er ».*

La Commission nationale note que la finalité du premier traitement institué par l'article 3, point 2° de l'avant-projet de règlement grand-ducal (c'est-à-dire, le traitement instauré par le nouvel article 12*bis*, paragraphe 1 du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers) est également indiquée. Ainsi, *« la SNCA est autorisée à accéder aux données et à y effectuer des requêtes automatisées en temps réel »* uniquement *« aux fins de vérification de l'accomplissement des exigences*

[122] Article 4, 8) du RGPD.

dont question à l'article 10 » du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers.

Par contre, la finalité du second traitement institué par l'article 3, point 2° de l'avant-projet de règlement grand-ducal (c'est-à-dire, le traitement instauré par le nouvel article 12bis, paragraphe 2 du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers) n'est pas clairement définie. Comme indiqué plus haut, la Commission nationale rappelle qu'en l'absence de plus amples explications, elle ne saisit pas les réelles raisons d'accorder aux assureurs un accès aux données techniques des véhicules routiers « lorsqu'un nouveau contrat d'assurance à responsabilité est à conclure ». En effet, a priori, il revient en principe à l'assuré de fournir à l'assureur toutes les données nécessaires à la conclusion du contrat d'assurance, le cas échéant, par l'intermédiaire du garagiste/concessionnaire. La Commission nationale estime dès lors nécessaire que la finalité soit précisée, afin d'apprécier la nécessité et la proportionnalité du traitement de données.

4) <u>Origine des données et accès aux données</u>

La Commission nationale constate que l'origine des données auxquelles les différents acteurs peuvent accéder n'est pas toujours clairement définie et mériterait d'être précisée.

Dans le cas de l'accès institué par l'article 2 de l'avant-projet de règlement grand-ducal, qui modifie l'article 5 du règlement grand-ducal modifié du 26 janvier 2016 sur le contrôle technique des véhicules routiers, la Commission nationale comprend que les données proviennent des bases de données des compagnies d'assurances.

Par contre, dans le cas du premier traitement instauré par l'article 3, point 2° de l'avant-projet de règlement grand-ducal (c'est-à-dire, le traitement instauré par le nouvel article 12*bis*, paragraphe 1 du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers), l'origine des données n'est pas claire. Il ne ressort ainsi pas du texte à quelles données la SNCA a accès et auprès de qui la SNCA obtient ces données.

De même, concernant le second traitement instauré par l'article 3, point 2° de l'avant-projet de règlement grand-ducal (c'est-à-dire, le traitement instauré par le nouvel article 12*bis*, paragraphe 2 du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers), l'origine des *« données techniques des véhicules routiers »* n'est pas non plus indiquée.

Concernant les moyens d'accès, la Commission nationale remarque également qu'il est précisé, aux articles 2 et 3, point 2°, dernier alinéa de l'avant-projet de règlement grand-ducal que les accès auront lieu via une *« interface mise à disposition par le Centre des Technologies de l'Information de l'État »*. Par contre, concernant l'accès créé par l'article 3, point 2° second alinéa de l'avant-projet de règlement grand-ducal (c'est-à-dire, le traitement

instauré par le nouvel article 12bis, paragraphe 1 du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers), elle constate que le moyen d'accès n'est pas précisé.

5) Principe de minimisation des données

L'article 5.1 c) du RGPD dispose que les données à caractère personnel doivent être *« adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) »*.

Il résulte de ce principe que ne doivent être traitées que les données nécessaires à l'accomplissement de la finalité du traitement. En d'autres termes, il s'agit de ne pas donner l'accès à plus de données que celles nécessaires, respectivement à la SNCA, aux organismes de contrôle technique et aux assureurs, pour accomplir la finalité pour laquelle un accès leur est octroyé.

La Commission nationale tient à relever l'importance de ce principe. La manière dont est rédigé l'avant-projet de règlement grand-ducal ne lui permet cependant pas d'apprécier pleinement si ce principe de minimisation des données sera en l'espèce respecté.

6) Conservation des données

La Commission nationale tient à rappeler que, selon l'article 5.1 (e) du RGPD, les données à caractère personnel doivent être *« conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (…) »*.

En l'espèce, il ressort de l'exposé des motifs que les données consultables via l'interface informatique ne seraient pas conservées.

Ainsi décidé à Esch-sur-Alzette en date du 16 juillet 2018.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann
Présidente	Membre effectif	Membre effectif

Avis de la Commission nationale pour la protection des données à l'égard du projet de loi n° 7258 portant modification 1) de la loi modifiée du 25 février 1979 concernant l'aide au logement, 2) de la loi modifiée du 21 septembre 2006 sur le bail à usage d'habitation et modifiant certaines dispositions du Code civil, et 3) de la loi modifiée du 16 décembre 2008 concernant l'accueil et l'intégration des étrangers au Grand-Duché de Luxembourg, et à l'égard du règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14quater-1 et 14quater-2 de la loi modifiée du 25 février 1979 concernant l'aide au logement.

Délibération n° 450/2018 du 14 septembre 2018

Conformément à l'article 57, paragraphe 1er, lettre (c) du 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 »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») « conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».

Faisant suite à la demande lui adressée par Monsieur le Ministre du logement en date du 22 mars 2018, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi portant modification 1) de la loi modifiée du 25 février 1979 concernant l'aide au logement, 2) de la loi modifiée du 21 septembre 2006 sur le bail à usage d'habitation et modifiant certaines dispositions du Code civil, et 3) de la loi modifiée du 16 décembre 2008 concernant l'accueil et l'intégration des étrangers au Grand-Duché de Luxembourg, et des projets de règlements grand-ducaux afférents, déposé à la Chambre des Députés comme projet de loi n° 7258 en date du 7 mars 2018, et des projets de règlements grand-ducaux suivants :

- le projet de règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14*quater-1* et 14*quater-2* de la loi modifiée du 25 février 1979 concernant l'aide au logement, et
- le projet de règlement grand-ducal déterminant les critères minimaux de salubrité, d'hygiène, de sécurité et d'habitabilité auxquels doivent répondre les logements et chambres donnés en location ou mis à disposition à des fins d'habitation.

La CNPD limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par le chapitre Ier du projet de loi précité, qui porte modification de la loi modifiée du 25 février 1979 concernant l'aide au logement, et par le projet de règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14*quater-1* et 14*quater-2* de la loi modifiée du 25 février 1979 concernant l'aide au logement. Elle n'entend dès lors pas se prononcer au sujet du projet de règlement grand-ducal déterminant les critères minimaux de salubrité, d'hygiène, de sécurité et d'habitabilité auxquels doivent répondre les logements et chambres donnés en location ou mis à disposition à des fins d'habitation.

Il ressort de l'exposé des motifs qu'un des objectifs principaux du projet de loi sous objet consiste à aligner les dispositions relatives à l'aide au financement de garanties locatives à celles concernant la subvention de loyer. Le projet de règlement grand-ducal précité entend quant à lui préciser les mesures d'exécution relatives à l'aide au financement de garanties locatives.

La Commission nationale rappelle à cet égard qu'elle a émis deux avis relatifs à la loi du 9 décembre 2015 portant introduction d'une subvention de loyer et modifiant des dispositions diverses, en date du 21 juillet 2014 (document parlementaire n° 6542/06) et du 2 juillet 2015 (document parlementaire n° 6542/11).

Dans la mesure où le chapitre Ier du projet de loi sous examen entend plus particulièrement aligner le chapitre 2quater (articles 14*quater-1* à 14*quater-6*) de la loi modifiée du 25 février 1979 concernant l'aide au logement, sur les dispositions du chapitre 2*quinquies* (articles 14*quinquies* à 14*septies*) de la même loi, introduites par la loi du 9 décembre 2015 portant introduction d'une subvention de loyer, elle entend se référer à ses avis précités.

Certes, au contraire de ladite loi, le projet de loi sous examen ne prévoit pas d'échange de données entre le ministère du logement et d'autres ministères ou administrations. Il s'ensuit que les risques en matière de protection de la vie privée et des données à caractère personnel n'apparaissent pas aussi élevés que dans la solution retenue en matière de subventions de loyer. Cependant, il résulte implicitement du projet de loi sous examen la création d'un nouveau traitement de données à caractère personnel en vue de la gestion et du suivi administratif des dossiers des demandeurs d'aide au financement d'une garantie locative. Dans ce contexte, les services du ministre ayant le logement dans ses attributions seront amenés à traiter des données à caractère personnel aux fins de l'instruction d'une demande d'aide au financement d'une garantie locative.

Or, toute base juridique servant de fondement à un traitement de données à caractère personnel visé à l'article 6, paragraphe (1), point (c) ou (e) du RGPD, doit être accompagné de garanties appropriées en matière de protection des données. En particulier, suivant le paragraphe (3) de ce même article :

« (…) les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires 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 (…) ».

Afin de se conformer à cette obligation, les auteurs dudit projet de loi pourraient prendre l'exemple de l'article 14*sexies* de la loi du 9 décembre 2015 dont ressort la création d'un fichier de données à caractère personnel par le ministère du logement aux fins de l'instruction d'une demande de subvention de loyer ou en cas de réexamen du dossier (cet article prévoit également l'accès par le ou les gestionnaires du dossier du ministère du logement à certains fichiers d'autres administrations, ce qui n'est pas prévu dans le texte actuel du projet de loi).

L'article 6, paragraphe (3) du RGPD prévoit encore que *« (…) cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent 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 [du RGPD] (…) ».*

En vertu du principe de sécurité juridique, la Commission nationale recommande dès lors que les conditions, critères et modalités des traitements des données mis en œuvre par le ministère du logement en vue de la gestion et du suivi administratif des dossiers des demandeurs d'aide au financement d'une garantie locative soient précisés dans une mesure législative ou réglementaire, par exemple dans le projet de règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14*quater-1* et 14*quater-2* de la loi modifiée du 25 février 1979 concernant l'aide au logement. Les auteurs de ce projet de règlement grand-ducal pourraient s'inspirer du règlement grand-ducal du 9 décembre 2015 fixant les conditions et modalités d'octroi de la subvention de loyer prévue par la loi modifiée du 25 février 1979 concernant l'aide au logement, au sujet duquel la CNPD s'était également prononcée dans son avis du 2 juillet 2015 (document parlementaire n° 6542/11).

Il est vrai que le projet de règlement grand-ducal sous examen prévoit déjà implicitement dans son article 2 les catégories de données qui pourraient être traitées par le ministère du logement aux fins de l'instruction ou du réexamen d'une demande d'aide au financement d'une garantie locative, ainsi que leur origine. La CNPD regrette toutefois la formulation du paragraphe (2) de cet article 2 (*« Le demandeur fournit, sur demande du ministre, tous renseignements et documents nécessaires à l'instruction de sa demande »*), qui ne paraît guère conforme au principe de prévisibilité auquel doit répondre tout texte légal ou réglementaire, et laisse par ailleurs courir le risque que la personne concernée se voit obligée de devoir transmettre davantage de données à caractère personnel en

fonction de sa situation particulière, voire de l'appréciation personnelle de l'agent du ministère qui serait amené à traiter sa demande (situation qui serait susceptible de contrevenir au principe d'égalité devant la loi, consacré à l'article 10*bis* de la Constitution).

En l'espèce, la Commission nationale n'est pas en mesure d'apprécier si le principe de minimisation des données, selon lequel seules peuvent être collectées les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (cf. article 5 paragraphe (1) lettre (c) du RGPD) serait respecté. Or, en vertu de l'article 6 paragraphe (3) précité du RGPD et du principe de sécurité juridique, la CNPD est d'avis qu'il appartient au législateur de mettre en œuvre et d'appliquer concrètement le principe de minimisation des données, sans quoi la loi ne répondrait pas à l'exigence de précision et de prévisibilité auquel doit répondre un texte légal selon la jurisprudence de la Cour européenne des droits de l'Homme[123].

Par ailleurs, les auteurs du projet de règlement grand-ducal sous objet pourraient prévoir pour les mêmes raisons des dispositions relatives à la conservation des données visées à l'article 2 par les services du ministre ayant le logement dans ses attributions ainsi que concernant la sécurité et la confidentialité des données (un système de journalisation des accès (également appelé piste d'audit ou « audit trail ») pourrait par exemple être prévu afin de se prémunir contre les risques d'abus ou de détournement de finalité).

Ainsi décidé à Esch-sur-Alzette en date du 14 septembre 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	François Thill Membre suppléant

[123] Voir notamment Cour Eur. D.H., Affaire Libert c. France, 22 février 2018, paragraphe 43.

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal déterminant le contenu minimal du dossier individuel du patient hospitalier et du résumé clinique de sortie.

Délibération n° 481/2018 du 19 octobre 2018

Conformément à l'article 57 paragraphe (1) lettre (c) 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, et abrogeant la directive 95/46/CE (ci-après désigné « le RGPD »), chaque autorité de contrôle a pour mission de conseiller *« conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement »*. L'article 7 de la loi du 1ier août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

Par courrier en date du 8 juin 2018, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal déterminant le contenu minimal du dossier individuel du patient hospitalier et du résumé clinique de sortie (ci-après « le projet de règlement grand-ducal »).

D'après l'exposé des motifs, ce projet de règlement grand-ducal vise à uniformiser le contenu du dossier individuel du patient hospitalier (ci-après : « le dossier hospitalier »), ainsi que du résumé clinique de sortie. En effet, l'article 37 de la loi du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière prévoit la mise en place dudit dossier hospitalier qui est censé retracer, de façon chronologique et fidèle, l'état de santé du patient et son évolution au cours de la prise en charge. L'article en question précise que *« le contenu minimal du dossier individuel du patient hospitalier et du résumé clinique de sortie est déterminé par règlement grand-ducal, l'avis de la Commission nationale pour la protection des données ayant été demandé. »*

La Commission nationale note avec satisfaction que le projet de règlement grand-ducal sous avis précise le contenu du dossier hospitalier, un texte dont l'adoption avait déjà été prévue dans le cadre de la loi abrogée du 28 août 1998 sur les établissements hospitaliers[124], ainsi qu'à l'article 15 paragraphe (1) alinéa 2 de la loi modifiée du 24 juillet 2014 relative aux droits et obligations du patient[125] (ci-après : *« la loi modifiée du 24 juillet 2014 »). Ledit article prévoit par ailleurs que le règlement grand-ducal devrait aussi fixer « le format, les codifications, les standards et les normes à utiliser aux fins d'assurer l'interopérabilité, de faciliter la tenue de bases de données communes standardisées, de tableaux de bord, et de permettre à l'aide de techniques d'anonymisation la conservation et l'extraction de données relatives au fonctionnement, à la performance et à la gestion du système*

[124] L'ancien article 36, alinéa 8 de la loi modifiée du 28 août 1998 sur les établissements hospitaliers prévoyait ce qui suit : « Un règlement grand-ducal peut établir un modèle type du dossier et du résumé clinique. » Ladite loi a été abrogée par la loi du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière.

[125] Ledit alinéa prévoit ce qui suit : « Le contenu minimal du dossier patient tenu par les différentes catégories de professionnels de santé ainsi que ses éléments sont déterminés par règlement grand-ducal, l'avis de la commission nationale pour la protection des données ayant été demandé. »

de santé ainsi qu'à des fins statistiques, de recherche et d'amélioration continue. » La CNPD regrette que le projet de règlement grand-ducal d'exécution sous avis ne contienne aucune précision à cet égard.

Comme les dispositions de la loi modifiée du 24 juillet 2014 s'appliquent aussi au dossier hospitalier[126], la Commission nationale tient à renvoyer par ailleurs à son avis adopté le 28 octobre 2011 relatif à la loi prédite[127]. Ladite loi réglemente, entre autres, l'accès au dossier patient par le patient lui-même, par les différents professionnels de santé intervenant dans sa prise en charge, ainsi que par ses ayants droit en cas de son décès. L'exposé des motifs du projet de règlement grand-ducal sous avis précise dans ce contexte que les principes généraux applicables aux dossiers patients énoncés à la loi modifiée du 24 juillet 2014 *« s'appliquent aussi bien au contenu et aux données du dossier individuel du patient hospitalier qu'à ceux du dossier individuel du patient en milieu extrahospitalier. »*

La Commission nationale entend limiter ses observations aux dispositions du projet de règlement grand-ducal ayant trait au respect de la vie privée et la protection des données à caractère personnel. Elle se propose de suivre l'ordre de rédaction du projet de règlement grand-ducal dans le cadre de ses observations.

Ad article 1ier : Champ d'application

L'article 1ier du projet de règlement grand-ducal prévoit qu'un dossier hospitalier est créé pour *« chaque séjour ou prise en charge d'un patient en hospitalisation stationnaire ou de jour dans un hôpital »*. Même si le commentaire des articles précise dans ce contexte que les prises en charge ambulatoires à l'hôpital (des *« consultations, des examens ou procédures faisant appel au plateau technique hospitalier sans être associés à une hospitalisation stationnaire ou de jour »*) sont exclues du champ d'application du texte sous examen, il serait utile d'insérer une définition du terme « prise en charge » dans le corps du texte. A ce titre, la CNPD rappelle qu'elle avait déjà soulevé dans son avis émis le 5 avril 2018 concernant le projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé[128] la nécessité de définir ladite notion.

Par ailleurs, la Commission nationale a cru comprendre qu'un dossier hospitalier sera créé par chaque hôpital par patient pris en charge et qu'il n'y aura pas d'interconnexion ou d'accès aux dossiers hospitaliers des patients d'autres établissements hospitaliers. Or, l'exposé des motifs du projet de règlement grand-ducal précise ce qui suit *« : Il s'agit de donner au dossier toute son utilité, afin de favoriser son usage en tant qu'outil de communication entre les multiples intervenants du processus de prise en charge et, le cas échéant, au-delà d'un seul établissement hospitalier […] »*. Si un professionnel de santé, travaillant au sein d'un établissement hospitalier distinct de celui ayant initialement pris en charge le patient, intervient ultérieurement dans la prise en charge, est-ce que le système prévu lui permettrait d'accéder directement par voie électronique au dossier hospitalier de ce patient, même si ce dossier a été créé par un autre établissement hospitalier ?

[126] L'article 37 paragraphe (2) de la loi du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière prévoit ce qui suit : « Sans préjudice des dispositions particulières de la présente loi et de ses règlements d'exécution, les dispositions de la loi du 24 juillet 2014 relative aux droits et obligations du patient s'appliquent au dossier individuel du patient hospitalier. »
[127] Délibération n° 357/2011 du 28 octobre 2011.
[128] Délibération n° 242/2018 du 5 avril 2018, p.18.

L'article 15 paragraphe (3) de la loi modifiée du 24 juillet 2014 précise à cet égard que si *« plusieurs professionnels de santé, médecin ou non médecin, interviennent dans la prise en charge du même patient et ont recours à un dossier patient utilisé de façon partagée, ils sont dispensés de tenir à jour un dossier patient propre pour y consigner ou verser les éléments ou informations déjà valablement documentées. […] »* Or, ledit article n'est pas suffisant afin de régler un éventuel accès à un même dossier hospitalier d'un patient par différents professionnels de santé travaillant pour le compte d'établissements hospitaliers distincts. Si cet accès est une hypothèse envisagée par les auteurs du projet de règlement grand-ducal, la Commission nationale estime que les conditions et modalités d'accès devraient être spécifiquement détaillées dans le corps du projet de règlement grand-ducal.

La CNPD s'interroge dans ce contexte comment l'article 37 paragraphe (2) de la loi du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière et l'article 15 paragraphe (3) de la loi modifiée du 24 juillet 2014 s'articuleront avec les dispositions légales relatives au dossier de soins partagé et s'inquiète d'éventuelles incohérences ou incertitudes qui pourraient en résulter.

Ad article 2 : Identification du patient

L'alinéa 1ier du paragraphe 1ier de l'article 2 du projet de règlement grand-ducal sous avis prévoit que les professionnels de santé ou le personnel administratif doit s'assurer d'une identification univoque d'un patient lors de son admission *« selon les procédures arrêtées par l'hôpital »*. Or, pour des raisons de sécurité juridique et afin d'instaurer un régime uniforme pour l'ensemble des hôpitaux luxembourgeois, la Commission nationale est d'avis que le texte du règlement grand-ducal devrait préciser cette formulation plus que vague.

En effet, à la connaissance de la CNPD, les établissements hospitaliers ont accès au registre national des personnes physiques, institué par la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques, afin d'identifier de manière univoque les patients résidants au Luxembourg. A côté de ce procédé d'identification fiable, le texte du projet de règlement grand-ducal envisage-t-il de laisser aux établissements hospitaliers le choix d'utiliser d'autres procédés d'identification, le cas échéant, moins fiables ? Le texte sous avis mérite donc d'être clarifié à ce sujet.

Finalement, selon le paragraphe (3) de l'article sous examen, le directeur général de l'hôpital est à considérer comme responsable du traitement des données du dossier hospitalier. Néanmoins, dans son avis susmentionné du 28 octobre 2011 concernant la loi modifiée du 24 juillet 2014, la CNPD avait conclu que sont *« responsables conjoints du dossier médical les médecins qui alimentent le volet médical et les établissements hospitaliers sous la responsabilité de son directeur médical. »*[129] Ceci vaut d'autant plus pour les médecins qui exercent leur profession à titre libéral, conjointement à une activité conventionnée à un hôpital. Ainsi, elle recommande aux auteurs du projet de règlement grand-ducal de prendre en compte la notion de « responsabilité conjointe » introduite par le RGPD à l'article 26. Ledit article exige en son paragraphe 1ier

[129] Délibération n° 357/2011 du 28 octobre 2011.

que *« les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. »* La même recommandation a déjà été émise par la CNPD dans le cadre du projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé.[130]

Ad article 3 : Contenu du dossier individuel du patient hospitalier

L'alinéa 1ier de l'article 3 renvoie à l'annexe 1 du projet de règlement grand-ducal en ce qui concerne le contenu minimal du dossier hospitalier. De manière générale, la Commission nationale salue le degré de détail avec lequel les auteurs du projet de règlement grand-ducal sous avis précisent les données à caractère personnel que le dossier hospitalier doit contenir.

Ledit alinéa précise que ce dossier *« comporte au moins les éléments décrits dans l'annexe 1 »*, tandis que l'annexe en elle-même est intitulée *« contenu minimal du dossier individuel du patient hospitalier »*. Comme susmentionné, l'article 37 de la loi du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière prévoit que le *« contenu minimal du dossier individuel du patient hospitalier et du résumé clinique de sortie est déterminé par règlement grand-ducal […]. »* Il en ressort que la liste prévue à l'annexe 1 du projet de règlement grand-ducal n'est pas à considérer comme exhaustive et que d'autres données que celles y prévues pourraient figurer au dossier hospitalier. Néanmoins, la Commission nationale se demande si les différents hôpitaux pourraient décider, à leur gré, d'ajouter d'autres données à caractère personnel dans le dossier hospitalier. Elle tient à souligner dans ce contexte l'importance du principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre c) du RGPD exigeant que les données à caractère personnel doivent être *« adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. »*

En ce qui concerne plus spécifiquement les données des patients issues de l'imagerie médicale, la Commission nationale tient à relever que par des amendements adoptés par la Commission de la Santé, de l'Egalité des chances et des Sports en date du 4 juillet 2018 dans le contexte du projet de loi n° 7172[131], la section relative à la création d'un carnet radiologique électronique a été supprimée. En effet, la Commission parlementaire en charge du projet de loi a estimé *« que le but du projet d'un carnet radiologique électronique, lancé dans le cadre du Plan Cancer, était de diminuer l'exposition de la population aux rayons ionisants d'origine médicale en évitant, grâce aux informations contenues dans le carnet radiologique électronique, les redondances d'examens d'imagerie médicale et de médecine nucléaire non nécessaires et utiles à la prise en charge du patient.*

[130] Délibération n° 242/2018 du 5 avril 2018, p. 6 et 7.

[131] Nouvel intitulé du 5 juillet 2018 : Projet de loi 1. relative à la protection sanitaire des personnes contre les dangers résultants de l'exposition aux rayonnements ionisants et à la sécurité des sources de rayonnements ionisants contre les actes de malveillance ; 2. relative à la gestion des déchets radioactifs, du transport de matières radioactives et de l'importation ; 3. portant modification de la loi modifiée du 21 novembre 1980 portant organisation de la Direction de la santé.

Or, par d'autres projets en cours, les principaux objectifs du carnet radiologique peuvent également être atteints. Ainsi, l'accès aux comptes rendus d'examens d'imagerie médicale, aux images et aux doses est prévu à travers le dossier de soins partagé.

Dans ce contexte, la Fédération des hôpitaux luxembourgeois (FHL) a lancé le projet Anim.lu, un projet de mutualisation de l'archivage de l'imagerie médicale, dans le but de faciliter la gestion de la politique de rétention des images médicales et de mieux maîtriser l'évolution des coûts à long terme dans ce domaine.

Pour éviter la multiplication d'applications comportant partiellement des finalités similaires, il a été décidé d'arrêter le projet du carnet radiologique électronique. Cette décision suit ainsi également l'avis du Conseil d'État qui note une redondance de moyens par rapport au dossier de soins partagé. »[132]

Ainsi, la Commission nationale se demande si les auteurs du projet de règlement grand-ducal ont volontairement omis de mentionner dans la rubrique des données médicales et de soins prévues à l'annexe 1 du projet de règlement grand-ducal, lettre C, les données relatives à l'imagerie médicale en suivant l'avis précité de la Commission de la Santé, de l'Égalité des chances et des Sports, ou si par contre ces dernières sont comprises au point 9 de ladite rubrique visant les « avis médicaux des médecins, les rapports des réunions de concertation pluridisciplinaire en oncologie, ainsi que les actes médicaux réalisés durant le séjour datés et validés par leur prestataire de soins ». La Commission nationale propose aux auteurs de clarifier ceci dans le texte du projet de règlement grand-ducal sous examen.

Ad article 4 : Accessibilité du dossier et régularisation des inscriptions

La Commission nationale tient à rappeler qu'en vertu de l'article 32 du RGPD, 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 peuvent augmenter avec le recours accru à certaines nouvelles technologies par les professionnels de santé qui pourraient par exemple utiliser des dispositifs mobiles (tablettes) pour accéder aux dossiers hospitaliers de leurs patients.

Par ailleurs, la CNPD estime nécessaire de prévoir explicitement un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. Ainsi, à l'instar d'autres lois ou règlements grand-ducaux, il conviendrait de rajouter une disposition qui pourrait avoir la teneur suivante: *« L'accès aux dossiers hospitalier doit être conçu et implémenté 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*

[132] Amendements adoptés dans le cadre du projet de loi n° 7172 par la Commission de la Santé, de l'Egalité des chances et des Sports en date du 4 juillet 2018, p.69.

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 ».

Ainsi décidé à Esch-sur-Alzette en date du 19 octobre 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Hemmerling Membre suppléant

ANNEXES

5

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7217 instituant un Registre des bénéficiaires effectifs et portant 1° transposition des dispositions de l'article 30 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, telle que modifiée par la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018; 2° modification de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises et au projet de règlement grand-ducal portant exécution de la loi du 13/01/2019 instituant un Registre des bénéficiaires effectifs.

Délibération n° 486/2018 du 22 novembre 2018

Conformément à l'article 57, paragraphe 1er, lettre (c) du 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 »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Justice en date du 6 décembre 2017, la Commission nationale entend présenter ci-après ses réflexions et commentaires relatifs au projet de loi n° 7217 instituant un Registre des bénéficiaires effectifs et portant 1° transposition des dispositions de l'article 30 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, telle que modifiée par la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018; 2° modification de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises (ci-après « le projet de loi »).

Selon l'exposé des motifs, le projet de loi entend adapter la législation luxembourgeoise aux exigences internationales en matière de transparence des personnes morales qui découlent de l'article 30 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission (ci-après la « Directive 2015/849 »).

Le projet de loi vise à instituer un registre central concernant des bénéficiaires effectifs ayant pour mission la conservation et la mise à disposition des informations sur les bénéficiaires effectifs des personnes morales.

Par courriers du 3 juillet 2018 et du 4 octobre 2018, Monsieur le Ministre de la Justice a saisi la CNPD afin qu'elle se prononce sur les amendements gouvernementaux du projet de loi sous objet ainsi que sur le projet de règlement grand-ducal portant exécution de la loi du xx/xx/2018 instituant un Registre des bénéficiaires effectifs (ci-après « le projet de règlement grand-ducal »). La première série d'amendements vise à intégrer dans le texte du projet de loi, les changements apportés à la Directive 2015/849 par la Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/CE (ci-après « la Directive 2018/843 »).

La deuxième série d'amendements du 4 octobre 2018 vise à intégrer les commentaires du Conseil d'État.

Selon les commentaires généraux des amendements gouvernementaux, *« la principale évolution est l'ouverture au grand public de l'accès audit registre, sans devoir justifier d'un intérêt légitime. »*[133] En effet, alors que la Directive 2015/849 et le projet de loi initial prévoyaient un accès au registre par le public, cet accès était limité aux personnes pouvant démontrer un intérêt légitime. Soucieuse de vouloir contribuer *« à préserver la confiance dans l'intégrité des transactions commerciales et du système financier »*[134], la Directive 2018/843 ouvre l'accès au registre des bénéficiaires effectifs au grand public, *« sans condition de résidence ni d'intérêt spécifiques »*[135].

L'avis de la Commission nationale tient compte des amendements gouvernementaux et se réfère à la numérotation des articles du texte coordonné.

Ayant déjà été consultée par le ministère de la Justice au stade d'avant-projet de loi en question, la Commission nationale se limite à formuler les observations suivantes.

[133] Projet de loi n° 7217, doc. parl. n° 7217/09 page 2.
[134] Directive 2018/843, considérant 30.
[135] Projet de loi n° 7217, doc. parl. n° 7217/09 page 4.

I. Les rôles et responsabilités

La CNPD note que le ministre ayant la Justice dans ses attributions serait à considérer comme le responsable du traitement (article 5, paragraphe 1er du projet de loi). Le gestionnaire, à savoir le *« Luxembourg Business Registers »*, aurait la qualité de sous-traitant (article 5, paragraphe 2 du projet de loi). Le projet de loi précise encore que le gestionnaire n'est pas responsable du contenu de l'information inscrite (article 5, paragraphe 4), mais qu'il peut, lors de l'inscription des informations, refuser un dossier dans le cadre de la vérification de la déclaration et des pièces justificatives (article 7, paragraphe 1er du projet de loi). Par ailleurs, dans le cadre d'une déclaration, les pièces justificatives permettraient *« au gestionnaire de contrôler que les informations dont l'inscription et les modifications sont demandées correspondent bien aux pièces en question »*[136].

Tout comme le Conseil d'État, la CNPD considère que ces dispositions sont contradictoires. En effet, *« [s]'il vérifie la concordance des informations données avec les pièces justificatives, le gestionnaire du registre des bénéficiaires effectifs est responsable du contenu de l'information qu'il inscrit »*[137].

Par ailleurs, il ressort de l'article 5, paragraphe 1er, lettre (d) du RGPD, que le responsable du traitement doit veiller à ce que les données traitées soient exactes et, si nécessaire, tenues à jour. Le responsable du traitement serait dès lors responsable pour l'exactitude des données traitées, y compris l'inscription des données suivant la vérification de la concordance entre les données à inscrire et les pièces justificatives.

Au vu de ce qui précède, il importe de résoudre la contradiction entre ces articles et d'attribuer clairement la responsabilité en ce qui concerne l'exactitude des données contenues dans le registre.

II. Les entités immatriculées

La CNPD s'interroge sur l'inclusion de certaines organisations sur la liste des entités devant transmettre les informations sur les bénéficiaires effectifs au registre (article 1er, point 4 du projet de loi), par exemple les associations sans buts lucratifs ou bien des établissements publics de l'État et des communes (article 1er, points 7 et 11 de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises). Elle se demande notamment quelles personnes seraient considérées comme étant les bénéficiaires effectifs et quelles données seraient transmises au registre.

III. Les données conservées par les entités immatriculées

Les données relatives aux bénéficiaires effectifs, qui doivent être obtenues et conservées par les entités immatriculées, sont les informations indiquées à l'article 3 du projet de loi ainsi que des pièces justificatives. Ces informations doivent être exactes, adéquates et actuelles.

[136] Projet de loi n° 7217, doc. parl. 7217/00, p. 13.
[137] Projet de loi n° 7217, doc. parl. 7217/10, p. 6.

Ces informations doivent être fournies aux autorités compétentes et aux professionnels sur demande dans les conditions prévues par le projet de loi (articles 18 et 19 du projet de loi). Il convient de rappeler que les autorités nationales ne peuvent demander des informations que dans le cadre de l'accomplissement de leurs missions et compétences spécifiques en matière de lutte contre le blanchiment et contre le financement du terrorisme.

IV. Les données figurant au registre

Il ressort du projet de loi et du projet de règlement grand-ducal que les données traitées par le gestionnaire dans le cadre de la gestion du registre comprennent, au moins, les données figurant sur les demandes d'inscription en cours, acceptées et refusées, les données actuelles inscrites dans le registre et les données historiques et les pièces justificatives. Le projet de loi ne contient cependant pas une disposition prévoyant l'ensemble des données traitées par le gestionnaire. Or, selon l'article 5, paragraphe 1er, lettre (c) du RGPD, seules les données adéquates, pertinentes et nécessaires au regard des finalités poursuivies par le responsable du traitement doivent être collectées (principe de minimisation des données). La CNPD propose dès lors d'indiquer dans un article unique une liste exhaustive des données seront traitées par le gestionnaire. Elle s'interroge encore sur les « données historiques » et suggère de préciser cette notion.

En outre, l'article 4, paragraphe 3 du projet de loi stipule que la demande d'inscription des informations comprend les pièces justificatives qui seraient précisées par un règlement grand-ducal. L'article 5 du projet de règlement grand-ducal annexé aux amendements du 4 octobre 2018 précise qu'il s'agit des (a) *« pièces officielles permettant d'établir l'identité des bénéficiaires effectifs, accompagnées d'une traduction en langue française, allemande ou luxembourgeoise si les pièces officielles ne sont pas rédigées en caractères latins »*, (b) *« le cas échéant, de la demande de limitation »* et (c) « *le cas échéant, d'un document attestant que la société est cotée sur un marché réglementé… »*. La CNPD s'interroge sur la nécessité et la proportionnalité de la transmission d'une pièce d'identité au gestionnaire et de la conservation des pièces par ce dernier.

En effet, la Directive 2015/849 ne fait aucunement mention à des pièces justificatives dans le cadre des informations contenues dans le registre. Par ailleurs, comme soulevé ci-avant, le projet de loi prévoit une obligation d'obtention et de conservation des informations relatives aux bénéficiaires effectifs pour les entités immatriculées et une obligation de transmettre ces informations aux autorités nationales.

La CNPD est ainsi à se demander s'il est nécessaire que les pièces justificatives soient conservées au sein du registre, alors qu'une telle conversation impliquerait non seulement une multiplication des copies des documents, mais également une centralisation des données à caractère personnel relatives à un grand nombre de personnes concernées.

Elle rappelle à cet égard l'importance du principe de minimisation des données ainsi que le principe de proportionnalité et de nécessité, selon lequel tout traitement de données à caractère personnel doit être proportionné aux finalités à atteindre, compte tenu du risque que le traitement fait peser sur la vie privée des personnes concernées.

Afin de minimiser les traitements de données dans le cadre du présent projet de loi et étant donné que les pièces justificatives doivent être conservées par les entités immatriculées, la CNPD suggère dès lors de supprimer du projet de loi l'obligation pour les entités immatriculées de fournir des pièces justificatives avec la demande et l'obligation pour le gestionnaire de conserver ces pièces.

La CNPD note encore que ni la notion d' *« intérêts effectifs détenus »*, ni celle de *« l'étendue des intérêts effectifs détenus »* ne sont définies dans le projet de loi. Afin de définir clairement les informations qui doivent être conservées et de respecter ainsi le principe de minimisation des données, elle se rallie dès lors à l'avis du Conseil d'État et préconise de clarifier ces notions[138].

Finalement, en conformité avec le principe de minimisation des données et pour diminuer l'impact du registre public pour les personnes concernées, la CNPD préconise encore de suivre la recommandation du considérant 34 de la Directive 2018/843 qui précise que *« [l]es registres devraient faire apparaître clairement si le dirigeant principal a été identifié comme étant le bénéficiaire effectif uniquement ex officio et non pas du fait qu'il détient une participation ou exerce un contrôle par un autre moyen. ».*

V. L'accès aux données contenues dans le registre

a. Accès par le grand public

Il ressort de l'article 12 du projet de loi que *« l'accès aux informations visées à l'article 3, paragraphe 1er, points 1° à 8°, 12° et 13° est ouvert à toute personne »,* à savoir le nom et le(s) prénom(s), la (ou les) nationalité(s), le jour, le mois et l'année de naissance, le lieu et le pays de naissance ainsi que la nature et l'étendue des intérêts effectifs détenus.

Selon l'article 30, paragraphe 5, alinéa 2 de la Directive 2015/849, telle que modifiée par la Directive 2018/843, les seules données auxquelles le public devra avoir accès sont le nom, le mois et l'année de naissance, la nationalité, le pays de résidence ainsi que la nature et l'étendue des intérêts effectifs détenus. L'alinéa 3 dudit article permet aux États membres de donner accès à des informations supplémentaires, telles que *« la date de naissance ou les coordonnées »* des bénéficiaires effectifs. Il en résulte que les auteurs se sont prévalus de cette possibilité en permettant au grand public d'avoir accès, en sus des informations prévues à l'article 30, paragraphe 5, alinéa 2 de la Directive 2015/849, au jour et au lieu de naissance des bénéficiaires effectifs.

[138] Projet de loi n° 7217, doc. parl. n° 7217/10 page 5.

La mise à disposition de ces informations supplémentaires au grand public se justifierait, selon le commentaire des articles, par les mesures techniques et organisationnelles du registre. En effet, comme les professionnels auraient accès aux données visées à l'article 3, paragraphe 1er, points 1° à 8° et 12° à 13°, il serait difficile pour le gestionnaire de distinguer entre l'accès par les professionnels et par le grand public en cas de demande d'accès[139].

Or, l'article 5, paragraphe 1er, lettre (c) du RGPD prescrit que seules les données adéquates, pertinentes et nécessaires au regard des finalités poursuivies par le responsable du traitement doivent être traitées. Par ailleurs, selon l'article 25, paragraphe 2 du RGPD, le responsable du traitement doit *« mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées »* (protection des données par défaut). Il importe ainsi de limiter au stricte nécessaire les informations disponibles au public dès la conception du traitement. Une limitation de ces informations contribuerait à la protection des données des personnes concernées contenues dans le registre et coïnciderait avec le considérant 34 de la Directive 2018/843, selon lequel *« un juste équilibre devrait, notamment, être recherché entre l'intérêt du grand public à la prévention du blanchiment de capitaux et du financement du terrorisme et les droits fondamentaux des personnes concernées. L'ensemble des données devant être mises à la disposition du public devrait être limité, défini de manière claire et exhaustive, et être de nature générale, de manière à réduire au minimum le préjudice susceptible d'être causé aux bénéficiaires effectifs ».*

En tenant compte de ce qui précède, la CNPD estime dès lors nécessaire de supprimer le jour de naissance et le lieu de naissance des bénéficiaires effectifs de la liste des informations auxquelles le grand public aura accès.

b. <u>Modalités d'accès et de recherche</u>

L'article 30, paragraphe 5*bis* de la Directive 2015/849, telle que modifiée par la Directive 2018/843, précise que les États membres ont la possibilité *« … de conditionner la mise à disposition des informations conservées dans les registres nationaux visés au paragraphe 3 à une inscription en ligne et au paiement d'une redevance… ».*

L'article 13, paragraphe 2 du projet de loi, dans la version résultant des amendements gouvernementaux du 4 octobre 2018, précise que *« Le système informatique, par lequel l'accès au Registre des bénéficiaires effectifs des autorités visées à l'article 11 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. »*

[139] Projet de loi n° 7217, doc. parl. n° 7217/09, page 4.

L'article 13, paragraphe 1er du projet de loi amendé laisse à des règlements grand-ducaux le soin de régler les modalités d'accès au registre et les critères de recherche.

Le projet de loi et le projet de règlement grand-ducal créent des régimes distincts pour la consultation par les autorités nationales, d'une part, et par le grand public et les entités assujetties, d'autre part.

i. Les autorités nationales

L'article 8, paragraphes 1er et 2 du projet de règlement grand-ducal précise que la demande d'accès doit émaner du responsable de l'autorité et que les modalités d'accès doivent être fixées dans une convention signée entre l'autorité et le gestionnaire. Or, comme l'a précisé le Conseil d'État dans son avis du 7 juin 2016 sur le projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'État pour études supérieures, *« 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 »*[140]. Les éléments essentiels[141], les objectifs et les principes[142], dont notamment les modalités d'accès, doivent dès lors figurer dans la loi.

ii. Les entités assujetties et le grand public

Il ressort du projet de loi et du projet de règlement grand-ducal que la consultation du registre ne serait pas soumise à une inscription en ligne et que les mesures de sécurité décrites à l'article 13 du projet de loi ne s'appliqueraient pas dans le cadre de la consultation du registre par le grand public et par les entités assujetties.

La CNPD constate encore que le projet de règlement grand-ducal institue le principe de la gratuité de la consultation du registre (article 7) en soumettant uniquement la demande d'un extrait ou d'un certificat à l'acquittement des frais administratifs (article 9). Selon le commentaire des articles, la gratuité s'explique par *« la transparence qu'il entend créer. Une consultation payante pourrait en effet être perçue comme une barrière à la consultation. »*[143]

La CNPD regrette le choix des auteurs de ne pas soumettre l'accès au registre par les entités assujetties et le grand public à ces mesures de sécurité. En effet, si l'ouverture de ce registre au grand public se justifierait, selon le considérant 30 de la Directive 2018/843, entre autre, par le fait que *« l'accès du public aux informations sur les bénéficiaires effectifs permet un contrôle accru des informations par la société civile, notamment la presse ou les organisations de la société civile, et contribue à préserver la confiance dans l'intégrité des transactions commerciales et du système financier »*, il est néanmoins important de trouver un juste équilibre *« entre l'intérêt du grand public à la prévention du blanchiment de capitaux et du financement du terrorisme et les droits fondamentaux des personnes concernées »* (considérant 34).

[140] Avis du Conseil d'État du 7 juin 2016 relatif au projet de loi n° 6975 portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'État pour études supérieures, p. 4.
[141] Arrêt de la Cour constitutionnelle - Arrêts n° 00132 et 00133 du 2 mars 2018.
[142] Avis n° 52976 du Conseil d'État du 24 juillet 2018 relatif au Projet de règlement grand-ducal 1. modifiant le règlement grand-ducal modifié du 10 août 2005 relatif au fonctionnement du lycée-pilote, et 2. abrogeant le règlement grand-ducal du 27 août 2012 portant sur les classes de la division supérieure de l'enseignement secondaire dans le cycle de formation du lycée Ermesinde.
[143] Projet de règlement grand-ducal, page 8.

Cette ouverture du registre au grand public devrait ainsi être compensée par des sauvegardes que les États membres pourraient mettre en place *« dans le but d'assurer une approche proportionnée et équilibrée et de garantir les droits au respect de la vie privée et à la protection des données à caractère personnel »*, comme, par exemple, l'exigence d'une inscription en ligne et le paiement d'une redevance, ainsi que la mise en place d'un traçage des personnes ayant consulté le registre (considérant 36 de la Directive 2018/843).

La CNPD estime que ces mesures représentent des sauvegardes indispensables pour cadrer l'ouverture du registre au grand public avec la législation en matière de protection des données et pour contribuer à la balance entre l'objectif légitime de la lutte contre le blanchiment et les droits fondamentaux des personnes concernées.

Le traçage des personnes ayant consulté le registre est par ailleurs justifié pour répondre aux droits des personnes concernées (les bénéficiaires effectifs) qui leurs sont conférés par le RGPD, à savoir le droit à l'information (article 12 à 14 du RGPD) et le droit d'accès (article 15 du RGPD). En effet, ces droits garantissent aux personnes concernées d'être informé sur les destinataires de leurs données, respectivement d'avoir accès aux informations relatives aux destinataires. A ce titre, il est encore renvoyé aux observations formulées au point VII du présent avis.

La CNPD soulève à cet égard que d'autres États membres ont jugé opportun de soumettre l'accès au registre à l'acquittement des frais administratif (p.ex. la Belgique). Elle rappelle finalement l'avis du Conseil d'État, selon lequel *« les frais de fonctionnement de ce registre ne devraient pas exclusivement reposer sur l'entité immatriculée et que les personnes ayant accès à ce registre en application de l'article 13 contribuent également à ces frais de fonctionnement »*.

Comme soulevé ci-avant, les sauvegardes proposées par la Directive 2018/843, à savoir l'inscription en ligne, l'exigence du paiement des frais administratif et le traçage des personnes ayant procédées aux consultations pourraient empêcher une utilisation abusive de ce nouvel outil de transparence. La CNPD estime dès lors nécessaire de soumettre tout accès au registre, que ce soit par les autorités nationales, par les entités assujetties ou par le grand public, aux conditions prévues au paragraphe 2 de l'article 13 de la loi en projet.

c. Limitation de l'accès au registre

L'article 15 du projet de loi prévoit la possibilité pour les entités immatriculées ou les bénéficiaires effectifs de demander la limitation de l'accès aux données contenues dans le registre et décrit la procédure à suivre. Afin de prendre une décision, le gestionnaire consultera le ministère public et la police grand-ducale[144]. La CNPD se demande si le gestionnaire serait amené à transmettre des données au ministère public et comment se ferait cette transmission dans le cadre de sa vérification de la concordance entre les affirmations du demandeur et les données détenues par le ministère public et la police à des fins pénales? Par ailleurs, afin de fournir une réponse au gestionnaire, est-ce que le ministère public ou la police transmettraient des données qu'ils traitent au gestionnaire ?

[144] Projet de loi n° 7217, doc. parl. n° 7217/14, page 14.

Dans un souci de sécurité juridique, la CNPD estime nécessaire d'encadrer cette coopération entre les autorités, notamment en précisant si le régime général du RGPD et de la loi modifiée du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données ou si le régime spécifique de la loi du 1er août 2018 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[145] s'applique à cet échange d'information.

Par ailleurs, s'agissant d'une matière réservée à la loi, il convient de fixer les éléments essentiels de cette coopération dans la loi.

VI. La durée de conservation

Selon l'article 10 du projet de loi, les informations concernant les bénéficiaires effectifs sont conservées au sein du registre pendant cinq ans après la date de la radiation de l'entité immatriculée du Registre de Commerce et des Sociétés. Les amendements gouvernementaux du 4 octobre 2018 précisent que les pièces justificatives seraient conservées pendant cinq ans. La CNPD rappelle que les personnes concernées auraient la possibilité d'exercer leurs droits aussi longtemps que leurs données sont traitées.

Nonobstant sa recommandation de supprimer l'obligation pour les entités immatriculées de transmettre les pièces justificatives au registre et au cas où cette obligation serait maintenue dans le projet de loi, la CNPD estime nécessaire de préciser la date à partir de laquelle le délai de conservation de cinq ans commence à courir.

Par ailleurs, la CNPD s'interroge sur la conservation des données relatives aux personnes concernées qui cessent d'être des bénéficiaires effectifs des entités immatriculées.

Selon le paragraphe 4 de l'article 8 du projet de règlement grand-ducal, les autorités nationales auraient accès aux informations inscrites et historiques, à l'exception des pièces justificatives. Selon le commentaire des articles du projet de règlement grand-ducal, l'accès à ces informations serait nécessaire dans le cadre de procès pénaux afin de pouvoir retracer les bénéficiaires effectifs d'une société[146]. Si les données dites « historiques » ne seraient pas disponibles pour le public et les entités assujetties, les autorités nationales y auraient accès par contre. La CNPD s'interroge ainsi sur la durée de conservation de ces données. En effet, ni le projet de loi, ni le projet de règlement grand-ducal n'indiquent la durée de conservation des données des personnes concernées qui cessent d'être des bénéficiaires effectifs.

Or, conformément à l'article 5, paragraphe 1er, lettre (e) du RGPD, les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

[145] Loi qui transpose la directive (UE) n° 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.
[146] Projet de règlement grand-ducal, page 8.

Dès lors, afin de limiter l'impact que la conservation des données pourrait avoir pour les personnes concernées et pour respecter les principes de minimisation des données et de limitation de la conservation, la CNPD estime nécessaire de limiter la durée pendant laquelle les données historiques seront conservées et pourront être accédées et encore de limiter les autorités pouvant accéder aux données historiques aux seules autorités nationales figurant aux lettres (a) à (d) du point 5 de l'article 1er du projet de loi.

Par ailleurs, quelle serait la durée de conservation des données obtenues et conservées par les entités immatriculées ? Dans un souci de sécurité juridique, il convient de préciser le projet de loi à cet égard.

VII. Les droits des personnes concernées

Pour ce qui est du responsable du traitement du registre des bénéficiaires effectifs, à savoir le ministre ayant la Justice dans ses attributions, celui-ci collectera les données de manière indirecte et devra, dès lors, en principe fournir toutes les informations prévues à l'article 14 du RGPD endéans les délais prévus à l'article 14, paragraphe 3 du RGPD. En vertu de l'article 14, paragraphe 5, lettre (c) du RGPD, le responsable du traitement est exempté de cette obligation, si l'obtention ou la communication est prévue par la loi, qui doit prévoir *« des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée »*. Le considérant 38 de la Directive 2018/843 précise que *« les personnes physiques dont les données à caractère personnel sont conservées dans des registres nationaux en tant que bénéficiaires effectifs devraient être informées en conséquence »*.

En tenant compte de la publication des données contenues dans le registre et afin de protéger les intérêts légitimes des personnes concernées, la CNPD estime nécessaire de prévoir, à l'instar de l'article 21, alinéa 2 de l'arrêté royal belge du 30 juillet 2018 relatif aux modalités de fonctionnement du registre des bénéficiaires effectifs, que le gestionnaire devrait informer chaque personne physique individuellement de son inscription dans le registre. Les personnes concernées devraient également recevoir les autres informations indiquées à l'article 14, dont notamment les informations relatives à leurs droits, ainsi que les procédures applicables à l'exercice de ces droits, conformément au considérant 38 de la Directive 2018/843. Cette information devrait avoir lieu endéans un mois de l'inscription[147].

Il convient encore de souligner que les entités immatriculées, qui collectent les données directement auprès des bénéficiaires effectifs, ont l'obligation de fournir à ces derniers les informations figurant à l'article 13 du RGPD.

A titre d'information, la CNPD rappelle encore que l'exercice par les personnes concernées de leurs droits, tel que les droits d'accès, de rectification et d'effacement, est gratuit et que les personnes concernées peuvent exercer ces droits auprès de chacun des responsables du traitement traitant leurs données, y compris le ministre ayant la Justice dans ses attributions par le biais du gestionnaire[148]. Il convient aussi de mentionner qu'en vertu du droit

[147] Commission de la protection de la vie privée, avis n° 43/2018 du 23 mai 2018 portant sur un arrêté royal relatif aux modalités de fonctionnement du registre des bénéficiaires effectifs (CO-A-2018-031), page 8.
[148] RGPD, article 12, paragraphe 5.

d'accès, les personnes concernées pourront connaitre la source des données contenues dans le registre (article 15, paragraphe 1er, lettre (g) du RGPD). Ainsi, pour le cas où le registre contiendrait des données inexactes, la personne concernée pourrait demander d'où proviendraient ces données.

Le considérant 38 de la Directive 2018/843 spécifie encore que les États membres peuvent, *« afin de prévenir l'utilisation abusive des informations contenues dans les registres et de rééquilibrer les droits des bénéficiaires effectifs, mettre à la disposition du bénéficiaire effectif des informations relatives au demandeur ainsi que la base juridique pour sa demande »*.

Selon l'article 13, paragraphe 3 de la loi en projet, tel qu'amendé par les amendements gouvernementaux du 4 octobre 2018, *« aucune information sur une consultation des données par une autorité visée à l'article 11 ne peut être communiquée aux entités immatriculées ou aux bénéficiaires effectifs. Le gestionnaire s'assure que la consultation de données du registre est opérée sans en alerter l'entité immatriculée concernée ou ses bénéficiaires effectifs. »*

La CNPD estime que les mesures proposées au considérant 38 de la Directive 2018/843 constitueraient des garanties pour les personnes concernées et contribueraient à la protection de leurs droits au respect de la vie privée et à la protection des données. Ces mesures seraient encore conforme à l'article 25, paragraphe 1er du RGPD, qui stipule que le responsable du traitement doit implémenter, dès la conception d'un traitement et en cours de traitement, des mesures techniques et organisationnelles appropriées, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

Afin d'offrir des garanties appropriées aux personnes concernées et de permettre le traçage des consultations des données y contenues et la base légale de la consultation, la Commission nationale estime nécessaire, à l'instar de ses homologues belges et en conformité avec le prédit considérant de la Directive 2018/843, de compléter le texte du projet de loi afin de prévoir de manière explicite, la possibilité pour les personnes concernées de connaître toutes les autorités, organismes et personnes qui ont, au cours des six mois écoulés, consultés ou mis à jour leurs données à l'exception des autorités administratives et judiciaires chargées de la recherche et de la répression de la lutte contre le blanchiment[149].

Ainsi décidé à Esch-sur-Alzette en date du 22 novembre 2018.

La Commission nationale pour la protection des données

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

[149] Commission de la protection de la vie privée, avis n° 43/2018 du 23 mai 2018 portant sur un arrêté royal relatif aux modalités de fonctionnement du registre des bénéficiaires effectifs (CO-A-2018-031), page 4.

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal portant exécution de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

Délibération n° 489/2018 du 7 décembre 2018

Conformément à l'article 57 paragraphe (1) lettre (c) 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, et abrogeant la directive 95/46/CE (ci-après désigné « le RGPD »), chaque autorité de contrôle a pour mission de conseiller *« conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement »*. L'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

Par courrier du 12 octobre 2018, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal portant exécution de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies et abrogation du règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire (ci-après « le projet de règlement grand-ducal »).

Il ressort du commentaire des articles que ce projet de règlement grand-ducal vise à répondre aux exigences formulées à l'article 2, paragraphe (2), à l'article 3 paragraphe (1), à l'article 5 paragraphe (2), à l'article 7 paragraphe (3), ainsi qu'à l'article 10 paragraphe (2), alinéa 2 et paragraphe (3) de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique (ci-après : « la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies »).

Le projet de règlement grand-ducal sous avis a plus précisément comme objet de dresser une liste des maladies à déclaration obligatoire et des maladies présentant une menace grave pour la santé publique, ainsi que le délai endéans duquel la déclaration doit être faite au directeur de la Santé ou à son délégué (ci-après désigné sous « l'autorité sanitaire ») par les médecins, les médecins-dentistes et les responsables des laboratoires d'analyses médicales (article 1er du projet de règlement grand-ducal pris sur base de l'article 2, paragraphe (2), de l'article 3 paragraphe (1) et de l'article 5 paragraphe (2) de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies).

L'article 2 du projet de règlement grand-ducal sous avis vise d'un côté à fixer une liste des maladies pour lesquelles la souche isolée ou le matériel biologique est à transférer par le laboratoire d'analyses médicales après établissement du diagnostic au laboratoire national de référence, sans demande spécifique par l'autorité sanitaire, ainsi que les délais y afférents, tel que prévu par l'article 7 paragraphe (3) de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies. D'autre côté, l'article en cause détermine les souches bactériennes, virales ou parasitaires pour lesquelles un laboratoire national de référence peut être désigné (tel que prévu par l'article 10 paragraphe (3) de la loi en cause). Finalement, l'article 10 paragraphe (2), alinéa 2 de ladite loi quant à lui laisse le soin au règlement grand-ducal sous avis de prévoir un modèle d'un cahier de charge visant à réaliser l'appel à candidatures par le ministre ayant la Santé dans ses attributions pour désigner un laboratoire national de référence.

Les articles 3 et 4 de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies indiquent quelles données à caractère personnel les déclarations de telles maladies par les médecins, médecins-dentistes et les laboratoires d'analyses médicales à destination de l'autorité sanitaire doivent comporter.

Pour rappel, la Commission nationale a rendu, le 10 mai 2017[150], un avis relatif au projet de loi n° 7160 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique (ci-après « le projet de loi »)[151], devenu la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies. Dans ledit avis, la CNPD s'était souciée notamment du recours à des données nominatives sans mise en place de mesures d'anonymisation irréversible des données, du manque de précisions quant aux mesures de sécurité et à la durée de conservation des données à caractère personnel, ainsi qu'à l'obligation de respecter le droit à l'information des personnes concernées. Au vu de la teneur actuelle de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies, la Commission nationale constate qu'elle n'a malheureusement pas été suivie par le législateur dans la majorité de ses recommandations.

Dès lors, la Commission nationale saisit l'occasion de réitérer certaines observations ayant trait au respect de la vie privée et la protection des données à caractère personnel dans le cadre du projet de règlement grand-ducal sous avis qui concernent aussi la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies. Par ailleurs, comme son avis précité du 10 mai 2017 a été émis sur base de l'ancienne loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel,[152] elle tient à ajouter certaines observations se basant spécifiquement sur le RGPD.

1. Quant à la base de légitimité de la création d'un système centralisé des maladies infectieuses

D'après l'exposé des motifs du projet de loi n° 7160, ledit projet permet *« 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. »* L'exposé continue en ce sens qu'afin d'éviter des doubles notifications et de

[150] Délibération n° 401/2017 du 10 mai 2017.

[151] Nouvel intitulé entier du 8 mai 2018: « Projet de loi sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique et modifiant : 1. la loi modifiée du 29 avril 1983 concernant l'exercice des professions de médecin, de médecin-dentiste et de médecin-vétérinaire ; 2. la loi modifiée du 16 juillet 1984 relative aux laboratoires d'analyses médicales ; 3. la loi modifiée du 16 janvier 1990 relative aux dispositifs médicaux ; 4. la loi modifiée du 8 juin 1999 relative au Collège médical ; 5. la loi du jj/mm/aaaa sur les conditions d'hygiène et de salubrité relatives à la pratique des techniques de tatouage par effraction cutanée, du perçage, du branding, cutting, ainsi que du bronzage UV ».

[152] Ladite loi a été abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

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. »* En effet et comme susmentionné, la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies, qui est issue du projet de loi n° 7160, contient dans ses articles 3 et 4 une liste de données à caractère personnel que les déclarations de maladies par les médecins, médecins-dentistes et les laboratoires d'analyses médicales à destination de l'autorité sanitaire doivent comporter « au moins ». Il s'agit plus particulièrement du nom, prénom, adresse, date de naissance, sexe, diagnostic médical du patient, ainsi que pour les déclarations effectuées par les médecins et médecins-dentistes de la date des premiers symptômes et du diagnostic, du pays où la maladie a été contractée et, le cas échéant, de la source d'infection. Les déclarations des laboratoires d'analyses médicales contiennent par ailleurs la date et l'origine du prélèvement des analyses du patient.

Il convient de noter dans ce contexte que l'article 6 paragraphe (3) du RGPD, 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 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.

En qui concerne spécifiquement le traitement de catégories particulières de données à caractère personnel, le considérant (54) du RGPD reconnaît des hypothèses dans lesquels le traitement de catégories particulières de données à caractère personnel (données dites « sensibles ») *« peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. Un tel traitement devrait faire l'objet de mesures appropriées et spécifiques de façon à protéger les droits et libertés des personnes physiques ».*

En effet, outre l'hypothèse d'un consentement explicite de la personne (article 9 paragraphe (2) lettre a) du RGPD), plusieurs situations peuvent légitimer un traitement portant sur des catégories particulières de données à caractère personnel, en particulier des données de santé. C'est notamment le cas lorsque *« le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel »* (article 9 paragraphe (2) lettre i) du RGPD).

La Commission nationale estime que les traitements de données mis en œuvre dans le cadre de la création du système centralisé des maladies infectieuses (ci-après : « le système centralisé ») relèvent des motifs d'intérêt public dans le domaine de la santé publique visés à l'article 9 paragraphe (2) lettre i) du RGPD, à condition que

le droit national le prévoit et que cette législation prévoit de telles « *mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée* ».

L'article 6 paragraphe (3) du RGPD 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* ».

Le considérant (45) du RGPD précise qu'il devrait « *[…] appartenir au droit de l'Union ou au droit d'un État membre de déterminer la finalité du traitement. Par ailleurs, ce droit pourrait préciser les conditions générales du présent règlement régissant la licéité du traitement des données à caractère personnel, établir les spécifications visant à déterminer le responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal. […]* »

Le considérant (41) énonce encore que « *cette base juridique ou cette mesure législative 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.* »

Ainsi, la Commission nationale se doit de souligner 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 ». 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 ». « Le degré de précision requis de la « loi » à cet égard dépendra du sujet en question. »

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. »

Le Conseil d'État 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 (…). »

La CNPD ne peut dès lors que saluer que l'État luxembourgeois ait pris la décision de respecter les exigences développées ci-avant en légiférant en la matière. Si on se réfère donc à l'article 9 paragraphe (2) lettre i) du RGPD comme condition de licéité, il y a lieu de vérifier si le droit luxembourgeois prévoit des *« mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée »* telles qu'exigées par le RGPD. Or, comme la CNPD n'a pas été suivie dans le contexte de son avis du 10 mai 2017 émis dans le cadre du projet de loi n° 7160 susmentionné, elle tient à souligner encore une fois dans cet avis-ci quelles dispositions devraient figurer dans un texte légal (loi ou règlement grand-ducal), donc a priori dans le projet de règlement grand-ducal sous avis.

2. Quant aux données à caractère personnel destinées à figurer dans le système centralisé

A titre préliminaire, la Commission nationale tient à relever qu'elle a constaté que ni la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies, ni le projet de règlement grand-ducal sous avis ne prennent

position quant à l'identité du responsable du traitement des données contenues dans le système centralisé, qui est défini à l'article 4 point 7) du RGPD comme la *« personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. »* Or, comme déjà mentionné dans son avis du 10 mai 2017, la CNPD considère qu'il ressort implicitement des textes légaux susmentionnés que l'autorité sanitaire est à considérer comme responsable du traitement, sous condition que les médecins, médecins dentistes et les laboratoires d'analyses médicales ont pour unique charge d'alimenter indirectement le système centralisé par leurs déclarations, mais qu'ils n'ont pas d'accès direct aux données contenues dans ledit système. En ce qui concerne le traitement de données prévu à l'article 2 du projet de règlement grand-ducal sous examen (transfert de souche ou matériel biologique par le laboratoire d'analyses médicales au laboratoire national de référence), la Commission nationale se demande si le laboratoire national de référence agira en tant que sous-traitant[153] de l'autorité sanitaire ou si, par contre, ledit laboratoire assumera le rôle du responsable pour le traitement spécifique des échantillons biologiques ?

Par ailleurs, il convient de noter que l'article 2 du projet de loi n° 7160 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique avait initialement prévu d'indiquer dans les déclarations pour certaines maladies visées par un astérisque dans la version initiale du projet de règlement grand-ducal sous avis uniquement les initiales du patient. Le règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire, qui sera abrogé par le règlement grand-ducal qui va résulter de ce projet, contenait déjà dans son article 2 une disposition similaire qui avait la teneur suivante : *« Les maladies signalées par un astérisque (*) sont déclarées de façon anonyme par les lettres initiales du prénom, du nom patronymique et du sexe, suivies par l'année de naissance. »*

Or, par des amendements adoptés en date du 7 mars 2018 par la Commission de la Santé, de l'Egalité des Chances et des Sports, cette disposition a été supprimée *« afin d'éviter toute forme de stigmatisation. Ainsi, la déclaration se fait avec des données nominatives, permettant à l'autorité sanitaire d'écarter tous les doublons. »*[154] La CNPD ne peut pas suivre ce raisonnement. En effet, la pseudonymisation est une garantie appropriée en termes de protection des données et de la vie privée. Le fait de signaler les maladies de manière nominative, au contraire, a pour effet de stigmatiser les personnes atteintes de telle ou telle maladie. Déjà dans son avis du 10 mai 2017, la CNPD se demandait 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 l'autorité sanitaire. La Commission nationale tient donc à réitérer qu'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*

[153] Voir l'article 4 point 8) du RGPD pour la définition du sous-traitant *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. »*

[154] Voir les amendements adoptés en date du 7 mars 2018 par la Commission de la Santé, de l'Égalité des Chances et des Sports dans le cadre du projet de loi n° 7160 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique.

marquées d'un astérisque dans le projet de règlement grand-ducal, que la transmission systématique de l'adresse du patient n'est pas pertinente. »

Les articles 3 et 4 de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies contiennent néanmoins une liste des données nominatives que la déclaration obligatoire de certaines maladies par les médecins, médecins-dentistes et les laboratoires d'analyses médicales à destination de l'autorité sanitaire doit comporter « au moins ». Il en ressort que ladite liste n'est pas à considérer comme exhaustive et que d'autres données que celles y prévues pourraient figurer dans la déclaration. La Commission nationale se demande si dès lors les différents acteurs (médecins, médecins-dentistes et laboratoires d'analyses médicales) pourraient décider, à leur gré, de compléter leurs déclarations par d'autres données à caractère personnel. Elle tient à souligner dans ce contexte l'importance du principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre c) du RGPD exigeant que les données à caractère personnel doivent être *« adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »*, qui ne semble pas être respecté en l'espèce par la loi précitée.

Finalement, la Commission nationale considère qu'en vertu de l'article 32 du RGPD, il revient à l'autorité sanitaire de garantir un niveau de sécurité particulièrement élevé dont notamment en ce qui concerne la confidentialité des données des personnes concernées. Comme soulevé dans son avis du 10 mai 2017 et en l'absence de précisions concernant les mesures techniques et organisationnelles mises en place dans les textes légaux en cause, la Commission nationale n'est toujours pas en mesure d'apprécier si le dispositif envisagé satisfait aux exigences de sécurité des données traitées. Elle est d'avis qu'au vu de l'extrême sensibilité des données collectées, des mesures d'anonymisation irréversible des données, passé un certain délai, devraient être mis en place afin de garantir une meilleure protection des personnes à l'égard de leurs données à caractère personnel. La CNPD avait constaté dans son avis précité qu'elle *« 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. »* La pseudonymisation des données est en effet une des mesures de sécurité énumérées à l'article 32 lettre a) du RGPD.

La CNPD estime primordial de prévoir en la matière une obligation de pseudonymiser, puis d'anonymiser les données, à l'instar de la procédure de gestion des données prévue par le code de la santé publique français qui est beaucoup plus protectrice de la vie privée des personnes concernées que celle actuellement prévue par les textes légaux luxembourgeois. En effet, le système prévu en France est tel que les notifications de maladies graves contiennent un numéro d'anonymat établi par codage informatique irréversible à partir des trois premières lettres des nom, prénom, date de naissance et sexe de la personne et c'est le déclarant lui-même ou le médecin de l'agence régionale de santé désigné par le directeur général de l'agence qui établit la correspondance entre le numéro d'anonymat et les éléments d'identité de la personne. Ces derniers doivent assurer la conservation de ladite liste de correspondance, aux fins de validation et d'exercice du droit d'accès, dans des conditions garantissant la confidentialité des informations.[155]

[155] Article R3113-2, Paragraphe (1) point 2° et R3113-3, alinéa 2 du Code français de la santé publique.

En vertu de l'article R3113-2, paragraphe (2) du code français de la santé publique, des arrêtés du ministre chargé de la santé doivent fixer pour chaque maladie, entre autres et en fonction des nécessités de constatations et de suivi, *« la période, d'une durée maximale de cinq ans à compter de la date de notification, pendant laquelle est conservée la correspondance, mentionnée à l'article R. 3113-3, entre le numéro d'anonymat et les éléments d'identité de la personne. A l'issue de cette même période, le médecin de l'Agence nationale de santé publique supprime de la fiche les coordonnées du prescripteur et, le cas échéant, celles du responsable du service de biologie ou du laboratoire. »*

3. Quant au traitement de données génétiques

Contrairement au texte légal européen précédant, la directive 95/46 du 24 octobre 1995,[156] le RGPD contient une définition des « données génétiques ». En effet, son article 4 point 13) prévoit que les données génétiques sont des *« données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question. »*

L'article 2 du projet de règlement grand-ducal sous examen renvoie à l'annexe B qui établit une liste des pathogènes dont la souche ou le matériel biologique est à transférer par le laboratoire d'analyses médicales au laboratoire national de référence après l'établissement du diagnostic du patient sans demande spécifique par l'autorité sanitaire. Même si ledit article ne précise pas si l'envoi de ces échantillons biologiques devra être accompagné par d'autres données à caractère personnel du patient en cause, comme son nom, prénom et son adresse, la Commission nationale suppose que ceci est bel est bien le cas. Les différents laboratoires opèrent donc un traitement de données génétiques ; données particulièrement intimes et potentiellement discriminantes nécessitant une protection accrue. Comme mentionné sous le *« point 2. Quant aux données à caractère personnel destinées à figurer dans le système centralisé »*, la Commission nationale recommande aux auteurs du projet de règlement grand-ducal de préciser dans ce contexte le rôle du laboratoire national de référence, c'est-à-dire d'indiquer si ce dernier agit en tant que sous-traitant de l'autorité sanitaire, en tant que responsable du traitement, ou si la notion de « responsabilité conjointe » introduite par l'article 26 du RGPD est à prendre en compte.

La CNPD tient à souligner que des données à caractère personnel peuvent uniquement être collectées pour des *« finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités »* (article 5 paragraphe (1) lettre b) du RGPD). Elle se demande notamment quelles sont exactement les finalités poursuivies par le traitement susmentionné des données génétiques. Est-ce que l'objectif de ce transfert de données au laboratoire national de référence vise à garantir une meilleure prise en charge du patient en cause en analysant ses échantillons pour trouver le suivi médical le mieux adapté à sa maladie ? Ou est-ce que ledit laboratoire utilise les données à des fins de recherche scientifique ultérieur ? Dans ce dernier cas, nous tenons à souligner que les articles 63 à 65 de la loi du 1er août 2018 portant organisation de la Commission nationale

[156] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

pour la protection des données et du régime général sur la protection des données contiennent des conditions spécifiques à respecter par un responsable du traitement en cas de traitement de données personnelles à des fins de recherche scientifique.

Finalement, la Commission nationale s'interroge si les laboratoires nationaux de référence vont recourir à un tiers de confiance qui assurera la pseudonymisation des données à caractère personnel, donc des échantillons biologiques y stockées. En effet, le recours à un organisme tiers de confiance, distinct de l'organisme traitant les données et qui serait seul en mesure d'établir le lien entre des personnes et des données les concernant, est considéré comme une garantie supplémentaire de respect de la vie privée des personnes et de protection de leurs données personnelles.

4. Quant aux droits des personnes concernées et à la durée de conservation des données

Le chapitre III du RGPD accorde certains droits aux personnes concernées par un traitement de données à caractère personnel, tandis que son article 23 prévoit la possibilité pour l'Union européenne ou pour les États membres de limiter par la voie de mesures législatives la portée des obligations et desdits droits pour garantir par exemple des objectifs importants d'intérêt public général dans les domaines de la santé publique et de la sécurité sociale. Le paragraphe (2) de l'article 23 du RGPD contient une liste minimale de dispositions qu'une telle mesure législative limitative doit contenir, comme par exemple les finalités du traitement et les catégories de données concernées. Or, sur base de notre lecture du texte, le législateur luxembourgeois n'a pas prévu de limiter les droits des personnes concernées en la matière règlementée par la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies et par le projet de règlement grand-ducal sous avis, et de ce fait, les personnes concernées par les traitements de données à caractère personnel y prévus disposent intégralement de tous les droits prévus aux articles 12 à 22 du RGPD.

Lesdites personnes ont notamment le droit de recevoir certaines informations du responsable du traitement, soit au moment où les données en question sont directement obtenues auprès de la personne, soit au cas où les données ne sont pas collectées auprès de la personne concernée, au plus tard lorsque les données sont communiquées pour la première fois à un autre destinataire. Ainsi, au moment où l'autorité sanitaire obtient en sa qualité de responsable du traitement des déclarations des médecins, médecins-dentistes et des laboratoires d'analyses médicales qui contiennent des données à caractère personnel des patients en cause, ladite autorité est obligée d'informer les patients, entre autres, sur les finalités du traitement, les catégories de données traitées ou encore sur la source d'où proviennent les données en cause. La CNPD avait par ailleurs ajouté dans son avis du 10 mai 2017, qu'en sus de l'obligation d'information imposée à l'autorité sanitaire, *« 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. »*

Par ailleurs, la CNPD tient à souligner que l'article 5, paragraphe (1), lettre (e) du RGPD impose au responsable du traitement de veiller à ce que les données qu'il traite ne soient pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées. Or, ni la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies, ni le projet de règlement grand-ducal sous avis ne contiennent une disposition spécifique quant à la durée de conservation d'un côté des données à caractère personnel contenues dans le système centralisé et d'autre côté des échantillons biologiques stockés au laboratoire national de référence. Dans son avis du 10 mai 2017, elle a déjà soulevé la nécessité de prévoir les dispositions concernant la durée de conservation des données dans un texte légal. Ainsi, elle estime absolument nécessaire de préciser la durée de conservation des données dans ce projet de règlement grand-ducal. La Commission nationale tient à renvoyer dans ce contexte à ses considérations sous le « point 2. Quant aux données à caractère personnel destinées à figurer dans le système centralisé » concernant le système mis en place en France.

5. Quant à l'accessibilité au système centralisé et à la mise en place de mesures de sécurité appropriées

La Commission nationale tient à rappeler tout d'abord qu'en vertu de l'article 32 du RGPD, 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 sécurité et notamment de la confidentialité des données à caractère personnel constitue un enjeu majeur en cas de traitement de données sensibles (données de santé / données génétiques) dans la mesure où la divulgation de ces données pourrait causer un préjudice grave aux patients. Ces risques peuvent augmenter avec le recours accru à certaines nouvelles technologies par les professionnels de santé qui pourraient par exemple utiliser des dispositifs mobiles (tablettes) pour accéder aux dossiers de leurs patients, ainsi que pour envoyer des déclarations à l'autorité sanitaire. Elle tient à insister sur la nécessité de prévoir des mesures de sécurité à l'état de l'art et conformément à l'article 32 du RGPD, afin de protéger l'identité des patients, tout en permettant une surveillance et un suivi efficace en cas de maladies infectieuses déclarées. Comme soulevé sous le point *« 2. Quant aux données à caractère personnel destinées à figurer dans le système centralisé »,* elle insiste que des mesures de pseudonymisation avec une anonymisation subséquente irréversible soient mises en place.

La Commission nationale recommande dans ce contexte le recours à un tiers de confiance, distinct de l'organisme traitant les données et qui serait seul en mesure d'établir le lien entre des personnes et les données les concernant, qui assurera la pseudonymisation des données à caractère personnel. Le recours à un tiers de confiance est considéré comme une garantie supplémentaire de respect de la vie privée des personnes et de protection de leurs données personnelles. La CNPD est ainsi d'avis qu'une obligation de mettre en place des mesures de sécurité appropriées comme susmentionnées est absolument nécessaire en la matière, d'autant plus que le risque en cas d'attaque informatique extérieure est particulièrement élevé si des données de santé nominatives sont enregistrées dans un système centralisé.

Elle a constaté par ailleurs que l'article 5 de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies laisse la possibilité aux différents acteurs d'envoyer les déclarations en cause, entre autres, par téléfax.

Néanmoins, la Commission nationale est d'avis que le téléfax ne constitue pas a priori un moyen de communication sécurisé au regard de l'état de l'art pour transmettre des données nominatives hautement sensibles. Comme les téléfax se trouvent souvent au secrétariat d'une institution, ceci peut conduire à divulguer à des destinataires non habilités des informations couvertes par le secret médical et à porter ainsi gravement atteinte à l'intimité de la vie privée des personnes. Ainsi, la Commission nationale estime, sur base de recommandations émises par son homologue français, la Commission Nationale de l'Informatique et des Libertés (CNIL),[157] que l'autorité sanitaire doit mettre en place des mesures de sécurité adéquates, comme par exemple vérifier que le téléfax est situé dans un local physiquement contrôlé et accessible uniquement au personnel médical et paramédical et que l'impression d'un message est subordonnée à l'introduction d'un code d'accès personnel. Il convient de noter dans ce contexte que la législation française autorise la transmission des notifications de maladies graves uniquement par voie postale sous pli confidentiel portant la mention « secret médical » ou par télétransmission après chiffrement des données.[158]

Par ailleurs, la CNPD recommande aux auteurs du projet de règlement grand-ducal de préciser qui aura au sein de l'autorité sanitaire accès aux données figurant dans le système centralisé, 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. Dans ce même contexte, la CNPD se demande où seront stockées les données contenues dans le système centralisé. Est-ce que lesdites données restent sur les serveurs du Ministère de la Santé ou est-ce qu'elles seront stockées dans des serveurs d'un sous-traitant qui est, le cas échéant, établi en dehors de l'Union européenne ? Elle se pose la même question dans le contexte des échantillons biologiques. Est-ce que ceux-ci sont conservés au laboratoire national de référence ou est-ce qu'un transfert vers une infrastructure de bio-banque est prévu ?

Finalement, la CNPD estime nécessaire de prévoir explicitement un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. Ainsi, à l'instar d'autres lois ou règlements grand-ducaux, il conviendrait de rajouter une disposition qui pourrait avoir la teneur suivante: « L'accès au système centralisé doit être conçu et implémenté 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 ».

Ainsi décidé à Esch-sur-Alzette en date du 7 décembre 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Josiane Pauly Membre suppléant

[157] CNIL, « Données de santé, messagerie électronique et fax », 1er décembre 2015, disponible sous : https://www.cnil.fr/fr/donnees-de-sante-messagerie-electronique-et-fax.
[158] Article R3113-3, alinéa 1er du code français de la santé publique.

Avis de la Commission nationale pour la protection des données à l'égard du projet de loi n° 7126 relative aux sanctions administratives communales modifiant 1) le Code pénal, 2) le Code de procédure pénale, et 3) la loi communale modifiée du 13 décembre 1988.

Délibération n° 490/2018 du 7 décembre 2018

Conformément à l'article 57, paragraphe 1er, lettre (e) du 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 »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

Faisant suite à la demande lui adressée par Monsieur le Ministre de l'Intérieur en date du 2 mai 2018, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi relative aux sanctions administratives communales modifiant 1) le Code pénal, 2) le Code de procédure pénale, et 3) la loi communale modifiée du 13 décembre 1988, déposé à la Chambre des Députés comme projet de loi n° 7126 en date du 4 avril 2017 (ci-après « le projet de loi »).

L'objectif principal du projet de loi est de faire *« face au besoin des communes de disposer d'un instrument leur permettant de lutter contre la petite délinquance, les actes de vandalisme et autres incivilités que le droit pénal et les organes répressifs ne permettent plus d'endiguer efficacement (…) »*[159].

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) Article 7 du projet de loi : accès du fonctionnaire sanctionnateur au registre national des personnes physiques

Selon l'article 7 du projet de loi, le fonctionnaire sanctionnateur a accès « aux données pertinentes à cette fin » du registre national des personnes physiques dans le cadre de l'exercice de ses compétences. La CNPD partage l'avis du législateur que le fonctionnaire sanctionnateur devrait avoir accès uniquement aux données pertinentes dans

[159] cf. Exposé des motifs, page 1, cinquième paragraphe.

le cadre de l'exercice de ses compétences, c'est-à-dire aux données mentionnées dans le fichier des sanctions administratives communales, et non pas aux autres données comprises dans le registre national des personnes physiques (comme, par exemple, les données concernant la famille de la personne concernée).

II) Articles 18 et 19 et l'article 10 du projet de loi : Registres des sanctions administratives communales

Les articles 18 et 19 du projet prévoient la création de trois fichiers présentant des différences relatives au créateur du fichier. L'article 18 du projet de loi prévoit que le fonctionnaire sanctionnateur tient un « fichier des infractions dont les constats lui sont transmis » et l'article 19 du projet de loi prévoit que les communes et la Police grand-ducale tiennent un *« fichier des sanctions administratives ».*

Selon l'article 18 du projet de loi, le fichier du fonctionnaire sanctionnateur contient i) le nom, prénom, date de naissance, résidence habituelle et, le cas échéant, le numéro d'identification des personnes qui font l'objet du constat, ii) la nature des faits commis, et iii) les sanctions infligées.

Selon l'article 19 du projet de loi, le fichier de la Police grand-ducale contient i) le nom, prénom, date de naissance, résidence habituelle et, le cas échéant, le numéro d'identification des personnes qui font l'objet du constat, et ii) la nature des faits commis. Et le fichier des communes contient i) le nom, prénom, date de naissance, résidence habituelle et, le cas échéant, le numéro d'identification des personnes qui font l'objet du constat, ii) la nature des faits commis, et iii) la date de transmission du constat au fonctionnaire sanctionnateur.

Il en résulte que le fichier du fonctionnaire sanctionnateur est le seul fichier à contenir à la fois l'infraction et la sanction infligée. Par contre, l'article 10 du projet de loi prévoit que le fonctionnaire sanctionnateur transmet une copie de la décision à la commune concernée. La CNPD se demande si la copie de la décision envoyée à la commune va être liée au fichier de la commune ? Dans un cas pareil, il y aurait de fait création d'un casier judiciaire communal.

Plus généralement, la Commission nationale constate un parallélisme entre le casier judiciaire prévu par la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire et le fichier du fonctionnaire sanctionnateur (et, le cas échéant, le fichier de la commune). La CNPD s'interroge sur les modalités de fonctionnement du fichier du fonctionnaire sanctionnateur (et, le cas échéant, le fichier de la commune) qui s'apparente à un casier judiciaire au niveau communal. En effet, il existe des règles très spécifiques en relation avec l'inscription et la radiation des décisions de condamnations des ordres judiciaires dans le casier judiciaire mais le projet de loi reste muet sur les modalités de fonctionnement des fichiers en question.

Selon l'article 5 paragraphe (1) lettre (e) du RGPD, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Le projet de loi ne fait pas mention d'une durée de

conservation limitée de l'inscription d'une infraction dans ces fichiers. La CNPD tient à rappeler qu'une limitation de la conservation des données inscrites dans le fichier du fonctionnaire sanctionnateur (et, le cas échéant, le fichier de la commune) est indispensable. Au surplus, la Commission nationale se demande qui va fixer cette durée de conservation (le Ministre, les communes ou le fonctionnaire sanctionnateur) et qui va être responsable pour la radiation des données après l'écoulement du temps de conservation des données ?

En outre, il existe des règles spécifiques en relation avec l'accès aux données traitées dans le casier judiciaire prévu par la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire. Le projet de loi semble limiter l'accès au fichier du fonctionnaire sanctionnateur au fonctionnaire sanctionnateur lui-même mais en ce qui concerne le fichier de la commune, le projet de loi ne prévoit aucune limitation d'accès au niveau de la commune. La CNPD recommande vivement d'inscrire i) un accès restreint à ce fichier dans le projet de loi, et ii) des précisions concernant le droit d'accès de la personne concernée au fichier du fonctionnaire sanctionnateur (et, le cas échéant, au fichier de la commune).

Contrairement à l'avis complémentaire du Conseil d'État du 23 octobre 2018, la CNPD approuve la précision des données pertinentes prévues dans les articles 18 et 19 du projet de loi. Le principe de sécurité juridique est ainsi renforcé et le RGPD prévoit expressément la possibilité de telles précisions dans le droit national.

Ainsi, l'article 6, paragraphe (3) du RGPD prévoit que *« (...) cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent 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 [du RGPD] (...) ».*

Le Considérant (45) du RGPD précise par ailleurs aussi que *« (…) ce droit [national] pourrait préciser les conditions générales du présent règlement régissant la licéité du traitement des données à caractère personnel, établir les spécifications visant à déterminer le responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal. »*

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

Ainsi décidé à Esch-sur-Alzette en date du 7 décembre 2018.

La Commission nationale pour la protection des données,

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Josiane Pauly Membre suppléant

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal précisant les modalités de gestion de l'identification des personnes et les catégories de données contenues dans les annuaires référentiels d'identification des patients et des prestataires.

Délibération n° 491/2018 du 21 décembre 2018

Conformément à l'article 57 paragraphe (1) lettre (c) 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, et abrogeant la directive 95/46/CE (ci-après désigné « le RGPD »), chaque autorité de contrôle a pour mission de conseiller *« conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement »*. L'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

Par courrier du 8 octobre 2018, Monsieur le Ministre de la Sécurité sociale a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal précisant les modalités de gestion de l'identification des personnes et les catégories de données contenues dans les annuaires référentiels d'identification des patients et des prestataires (ci-après « le projet de règlement grand-ducal »). Ce projet est pris en application de l'article 60ter, paragraphe (2), alinéa 7 du Code de la sécurité sociale, introduit par la loi du 13 décembre 2017 modifiant certaines dispositions du Code de la sécurité sociale[160] et prévoyant qu'un *« règlement grand-ducal précise les modalités de gestion de l'identification et les catégories de données contenues dans les annuaires référentiels d'identification. »* Dans son avis du 2 décembre 2016 relatif au projet de loi n° 7061 devenu la loi du 13 décembre 2017,[161] la CNPD avait souligné l'importance de conférer une base légale au dispositif d'identitovigilance développé par l'Agence nationale des informations partagées dans le domaine de la santé (ci-après désignée « l'Agence eSanté ») d'une part, et aux annuaires référentiels d'identification des patients et des prestataires de soins de santé, d'autre part, en permettant de garantir les objectifs de sécurité et de qualité de l'information qui sous-tendent la mise en place desdits outils par l'Agence eSanté.

La Commission nationale entend limiter ses observations aux dispositions du projet de règlement grand-ducal ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel. Elle se propose de suivre l'ordre de rédaction du projet de règlement grand-ducal pour formuler ses recommandations.

[160] Loi du 13 décembre 2017 modifiant certaines dispositions du Code de la sécurité sociale (Mémorial A-2017-1063 du 15 décembre 2017, p. 1, doc. parl. 7061).
[161] Délibération n° 1005/2016 du 2 décembre 2016.

Ad article 1er

L'alinéa 1er de l'article sous revue prévoit l'obligation de l'Agence eSanté de mettre en place une procédure d'identification des personnes et d'administration des annuaires référentiels d'identification des patients et des prestataires de soins de santé. L'alinéa 2 de l'article 1er du projet de règlement grand-ducal prévoit plus précisément la mise en place de règles de traçage des accès à la plateforme électronique nationale d'échange et de partage de données de santé (ci-après : « la plateforme »). Néanmoins, au vu du titre du projet sous avis, la CNPD ne peut que se rallier à l'avis du Conseil d'État du 27 novembre 2018 qui s'est demandé si *« la disposition sous revue ne dépasse pas le cadre tracé par l'article 60ter, paragraphe 2, du Code de la sécurité sociale dans la mesure où la plateforme constitue le point d'entrée à plusieurs systèmes de traitement de données dont celui qui fait l'objet du règlement grand-ducal en projet. »*[162] En effet, ladite plateforme permet aux professionnels de soins de santé et aux patients d'accéder à un ensemble de services proposés par l'Agence eSanté, comme par exemple le dossier de soins partagé.

Indépendamment des considérations susmentionnées, la Commission nationale estime que l'article 1er du projet de règlement grand-ducal mériterait d'être clarifié et précisé. Tout d'abord, son alinéa 2 dispose que certaines informations relatives à l'utilisateur ayant accédé à la plateforme doivent être retracées. Or, le terme « utilisateur » n'étant pas défini, la CNPD se demande si ce dernier vise l'ensemble des professionnels de santé énumérés à l'article 61 du Code de la sécurité sociale, personnes physiques, les utilisateurs-salarié d'un professionnel de santé, personne morale (collectivité de santé) ou uniquement le professionnel de santé, personne morale (collectivité de santé), voire d'autres acteurs ? Le Conseil d'État ajoute dans son avis du 27 novembre 2018 la question si l'Agence eSanté est aussi à considérer « comme utilisateur et si les accès et actions de cette dernière devraient dès lors également être retracés. » Ensuite, l'alinéa 3 de l'article 2 accorde la possibilité à l'Agence eSanté de communiquer des informations aux utilisateurs de la plateforme au moyen de fichiers électroniques, sans précisant en quoi consistent ces « informations ». La CNPD tient à insister qu'au cas où le terme « informations » englobe aussi des données à caractère personnel, qui sont définies par l'article 4 point 1) du RGPD comme « toute information se rapportant à une personne physique identifiée ou identifiable », toutes les dispositions du RGPD seront applicables à ces transferts de données.

Ainsi, pour des raisons de sécurité juridique, la Commission nationale est d'avis que le texte du règlement grand-ducal sous avis devrait préciser davantage les notions « utilisateur » et « informations ».

Par ailleurs, le commentaire des articles précise qu'afin d'identifier les professionnels de santé souhaitant se connecter à la plateforme, l'Agence eSanté attribue un identifiant électronique unique à chaque professionnel de santé et collectivité de santé dans le cadre des échanges électroniques à travers la plateforme. La CNPD considère qu'il est primordial que chaque professionnel de santé travaillant dans une collectivité de santé a un identifiant

[162] Avis n° CE 53.106 du Conseil d'État du 27 novembre 2018.

personnel et qu'il n'est pas admissible qu'une telle collectivité dispose d'un identifiant en commun. Déjà dans son avis du 5 avril 2018 relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé, la Commission nationale avait insisté sur l'importance de prévoir une *« obligation pour les collectivités de santé de mettre en place des systèmes de traçage des accès qui sont nominatifs et individuels. »*[163]

Ad article 2

L'article 60*ter* paragraphe (2) alinéa 4 du Code de la sécurité sociale énumère explicitement à quelles données à caractère personnel de l'article 5 paragraphe (2) de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques l'Agence eSanté peut recourir pour peupler et mettre à jour l'annuaire référentiel d'identification des patients, encore appelé Master Patient Index (MPI). L'Agence eSanté peut de même utiliser les données d'affiliation fournies par le Centre commun de la sécurité sociale.

L'article 2 alinéa 1er du projet de règlement grand-ducal reprend de manière exacte l'ensemble des données et catégories de données à caractère personnel prévu par l'article susmentionné du Code de la sécurité sociale.

Par ailleurs, l'alinéa 2 de l'article 2 du projet de règlement grand-ducal sous examen fixe la durée de conservation des données contenues dans l'annuaire référentiel d'identification des patients à un maximum de 10 ans *« à compter du jour où l'identification du patient, respectivement du prestataire de soins devient sans objet dans le cadre des traitements de données visés à l'article 60ter du Code de la sécurité sociale et ce sans préjudice des dispositions fixant une durée de conservation particulière des données traitées sur la plateforme électronique nationale d'échange et de partage de données de santé par l'Agence. »* La CNPD tient à rappeler dans ce contexte l'exigence légale prévue à l'article 5 paragraphe (1) lettre e) du RGPD de ne pas conserver les données à caractère personnel sous une forme permettant l'identification des personnes concernées pendant une excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Sur base de la lecture seule de l'alinéa en cause, il n'est pas possible pour la CNPD de cerner quel est le point de départ exact du délai de 10 ans.

Ainsi, pour fixer le déclenchement de la durée de conservation maximale de 10 ans, la CNPD se rallie à l'avis du Conseil d'État ayant recommandé aux auteurs du projet de règlement grand-ducal de s'inspirer des points de départ prévus dans le projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé pour la suppression des données, à savoir le décès du patient et la fermeture des applications de la plateforme. La CNPD estime donc nécessaire de décrire de manière concise dans le corps du texte du projet de règlement grand-ducal sous avis quel est le point de départ exact du délai de 10 ans.

[163] Délibération n° 242/2018 du 5 avril 2018.

Outre la question du début précis de la période de conservation, la Commission nationale se demande de manière générale si le délai de 10 ans est justifié par rapport aux finalités poursuivies par la mise en place de l'annuaire référentiel d'identification des patients. Les auteurs du projet de loi n° 7061 devenu la loi du 13 décembre 2017 modifiant certaines dispositions du Code de la sécurité sociale, décrivaient les finalités dudit annuaire, ainsi que de l'annuaire référentiel d'identification des prestataires de soins de santé de la manière suivante : *« Une gestion sécurisée des identités s'impose non seulement pour les accès des patients et des prestataires à la plateforme nationale et au dossier de soins partagé mais, de manière générale, dans tous les projets informatiques à envergure nationale visant un échange sécurisé ou une meilleure utilisation des données relatives à la santé. A cette fin, l'Agence eSanté a mis en place un système de surveillance et de prévention des erreurs et risques liés à l'identification des patients et des prestataires pour gérer la qualité et la fiabilité des informations traitées dans les services déployés. Il est essentiel de garantir qu'un même patient ou prestataire est identifié de manière unique dans tout l'écosystème de la plateforme et dans les communications réciproques avec les systèmes d'informations des acteurs du domaine de la santé et des soins. »*[164] Le commentaire des articles du règlement grand-ducal sous avis précise à cet égard que la durée de conservation vise à s'aligner à la durée maximale pendant laquelle les professionnels et les établissements de santé, utilisant une application de la plateforme pour la gestion de leurs dossiers patients, conservent en pratique les données. Le commentaire continue en ce sens que les *« données pourront toutefois être supprimées dans un délai plus court si leur conservation n'est plus justifiée au regard des besoins d'interaction de l'annuaire avec les applications de la plateforme. »*

Or, en considérant que l'annuaire référentiel d'identification des patients ne se substituera pas aux dossiers des patients tenus par les médecins, établissements hospitaliers et autres professionnels de santé, la Commission nationale considère qu'une durée de conservation de dix ans après le décès d'un patient ou la fermeture des applications de la plateforme apparaît comme excessive au regard des finalités précitées dudit annuaire.

Ad article 3

Sur base de l'article 60*ter* paragraphe (2) alinéas 5 et 6 du Code de la sécurité sociale, l'article 3 du projet de règlement grand-ducal énonce les données à caractère personnel incluses dans l'annuaire référentiel d'identification des prestataires de soins de santé. En s'alignant sur la durée de conservation des données contenues dans l'annuaire référentiel d'identification des patients, l'alinéa 2 de l'article 3 prévoit la même disposition quant à la durée de conservation de maximum 10 ans à compter du jour ou l'identification du patient, respectivement du prestataire de soins devient sans objet. La CNPD renvoie dans ce contexte à ses commentaires sous le point *« Ad article 2 »* concernant le point de départ de la période de conservation, ainsi que la durée en elle-même.

[164] Commentaire des articles du projet de loi n° 7061 modifiant certaines dispositions du Code de la sécurité sociale, déposé le 13 septembre 2016.

Ad article 4

D'après l'article 4, alinéa 1er du règlement grand-ducal sous examen, l'Agence eSanté informe les patients et prestataires de soins de santé sur la nature et la finalité des données inscrites dans les annuaires respectifs, ainsi que sur l'existence de leur droit d'accès, d'information et de rectification pendant toute la durée du traitement des données. La CNPD tient néanmoins à préciser tout d'abord que le droit à l'information émane directement des articles 13 et 14 du RGPD et que ces dispositions ne doivent pas être reprises dans un texte légal national, sauf lorsque le législateur national entend limiter les droits des personnes concernées conformément à l'article 23 du RGPD. Indépendamment de cette considération, les auteurs devraient prendre en considération l'ensemble des informations prévues aux articles susmentionnés du RGPD comprenant par exemple, en sus de ce qui est mentionné à l'article 4, alinéa 1er du projet de règlement grand-ducal, les coordonnées du délégué à la protection des données, les destinataires ou les catégories de destinataires des données à caractère personnel, la durée de conservation des données à caractère personnel, ainsi que le droit d'introduire une réclamation auprès de la CNPD.

Par ailleurs, selon l'article 4, alinéas 2 à 4 du projet de règlement grand-ducal, l'Agence eSanté transmet les demandes d'accès et de rectification aux données par les patients et prestataires de soins de santé aux organismes respectifs compétents en la matière, c'est-à-dire au Centre commun de la sécurité sociale, aux instances prévues par la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, ainsi qu'au Ministre ayant la Santé dans ses attributions et à la Caisse nationale de santé.

En ce qui concerne les demandes de rectification, la CNPD peut comprendre que dans un but de simplification administrative, l'Agence eSanté transmet lesdites demandes directement aux organismes se trouvant à l'origine des données. Néanmoins, comme le souligne à juste titre le Conseil d'État dans son avis du 27 novembre 2018, l'Agence eSanté est le *« responsable du traitement, et ce indépendamment de l'origine des données. Le Conseil d'État attire l'attention des auteurs sur le fait que la disposition sous avis pourrait être comprise comme conférant à l'Agence la possibilité de se décharger des obligations prévues par le règlement européen. […] »* Ainsi, en cas de demande de rectification de données par un patient ou un prestataire de soins de santé, l'Agence eSanté est tenue de s'assurer en vertu de l'article 16 du RGPD que les données inexactes sont corrigées dans ses propres fichiers, dont notamment les annuaires référentiels d'identification des patients et des prestataires de soins de santé.

Par ailleurs, en cas de demande d'accès par un patient ou un prestataire de soins de santé aux données détenues par l'Agence eSanté, cette dernière est obligée en sa qualité de responsable du traitement et en vertu de l'article 15 du RGPD d'y répondre sans intermédiaire dans un délai d'un mois à compter de la réception de la demande, prolongeable de deux mois compte tenu de la complexité et du nombre de demandes (article 12 paragraphe (3)

du RGPD), sauf à considérer le Centre commun de la sécurité sociale, les instances prévues par la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, ainsi que le Ministre ayant la Santé dans ses attributions et la Caisse nationale de santé comme sous-traitants de l'Agence eSanté.

Finalement, la CNPD tient à souligner que cette possibilité offerte aux patients et professionnels de soins de santé d'exercer leurs droits de rectification via l'Agence eSanté est sans préjudice de l'article 37 de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques prévoyant en son paragraphe (1), alinéa 2 que toute personne peut demander la rectification de ses données « soit directement au guichet de la commune sur base d'un formulaire, soit par lettre simple ou par voie électronique au ministre pour les données inscrites sur le registre national ou au bourgmestre pour les données inscrites sur le registre communal. […] »

Ainsi décidé à Esch-sur-Alzette en date du 21 décembre 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Josiane Pauly Membre suppléant

brain&more

CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

1, avenue du Rock'n'Roll - L-4361 Esch-sur-Alzette
Téléphone : +352 26 10 60-1 - Fax : +352 26 10 60-29
www.cnpd.lu