RAPPORT ANNUEL 2020

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

La CNPD a comme objectif de protéger la vie privée des citoyens et de veiller au respect de la législation en matière de protection des données qui lui confie les missions suivantes :

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 visites sur place portant sur la protection des données suite à des réclamations ou de sa propre initiative ;
- les audits portant sur la protection des données suite à des réclamations ou de sa propre initiative ;
- 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 potentielles violations 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 agents 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, intègre et visible. Elle promeut une atmosphère positive et respectueuse.

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 l'environnement socioéconomique luxembourgeois.

TABLE DES MATIÈRES

AVANT-PROPOS

1

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

Depuis le mois de mars 2020, la vie quotidienne des Luxembourgeois est bouleversée par la pandémie du coronavirus (COVID-19).

Que ce soit dans la sphère privée ou professionnelle, la pandémie a eu un impact sur tous les aspects de notre vie. Des pratiques jusqu'ici peu répandues comme le télétravail, les réunions et les conférences en ligne ou l'enseignement à distance se sont mises en place en raison du confinement.

Pour permettre la continuité de leurs activités tout en respectant les mesures de distanciation sociale décidées par le gouvernement, les acteurs de la vie économique et sociale, tout comme les citoyens ont recouru massivement aux outils numériques. En plus des réseaux sociaux et des médias en ligne déjà solidement ancrés dans les habitudes de la grande majorité des citoyens avant la pandémie, les plateformes de vidéoconférence se sont généralisées dans le monde du travail, du moins pour les activités qui le permettaient.

Comme la plupart des organisations qui pouvaient le faire, la CNPD a basculé dans le télétravail dès le 17 mars 2020. Cette transition a été rapide et efficace et s'est déroulée sans incidents majeurs, ce qui a permis à la CNPD d'assurer sans interruption la continuité de ses missions.

La transformation digitale a eu un coup de pouce en quelques mois et le déploiement rapide vers des solutions numériques a bien évidemment conduit à une augmentation du traitement de données personnelles.

Partout en Europe, les gouvernements et les organisations publiques et privées ont pris des mesures pour enrayer et atténuer la prolifération du COVID-19. Des traitements de données inédits ont été mis en œuvre pour répondre ponctuellement à l'urgence sanitaire comme par exemple le « contact tracing », la mesure de la température corporelle à l'entrée de locaux ou le « large scale testing » de la population.

La CNPD, de concert avec ses homologues européens, a joué un rôle important pour assurer que le déploiement de ces mesures prises se fasse dans le respect des règles en matière de protection des données.

En effet, même en cette période hors du commun, les responsables de traitement de données et les sous-traitants doivent garantir la protection des données à caractère personnel des personnes concernées. Ceci est valable en particulier pour les données de santé qui se trouvent au cœur de la crise sanitaire. Leur utilisation impose le respect des principes essentiels protégeant la vie privée et la confidentialité des informations médicales qui concernent les citoyens.

Au Luxembourg et en Europe, le débat sur la question de la protection des données et la protection de la vie privée dans le contexte de la pandémie COVID-19 a été animé, ce qui traduit une grande sensibilité au sein de la société civile, de l'économie et de la politique sur ces sujets.

Le Gouvernement, conscient des enjeux, a sollicité l'avis de la CNPD pour les projets de loi COVID-19 successifs. La Commission nationale a, à chaque fois, avisé rapidement ces projets de loi en pointant la nécessité de la mise en place de garanties destinées à la protection des données des citoyens.

Malgré la situation, le projet d'aménagement des nouveaux locaux n'a connu que peu de retard. Ainsi, la CNPD a pu réaliser son déménagement sur le site de Belval en juin.

AVANT-PROPOS

1

LE RGPD - 2 ANS APRÈS

Alors que l'actualité internationale en matière de protection des données a en 2020 été dominée par l'invalidation du « Privacy Shield » (qui encadrait le transfert de données entre l'UE et les États-Unis) par la Cour de justice de l'Union européenne (affaire « Schrems II ») ainsi que par le Brexit, un autre point à relever est le rapport d'évaluation du règlement général sur la protection des données (RGPD)[1] publié par la Commission européenne deux ans après l'entrée en application du règlement.

Ce rapport a fait apparaître que le RGPD a atteint la plupart de ses objectifs, notamment en conférant aux citoyens un ensemble solide de droits et en créant un nouveau système européen de gouvernance et de contrôle de son application. Le RGPD s'est révélé être un outil souple à l'appui de l'élaboration de solutions numériques dans des circonstances imprévues telles que la crise du COVID-19. Le rapport a par ailleurs constaté que les entreprises développent une culture du respect de la réglementation et font de plus en plus valoir comme un avantage concurrentiel le niveau élevé de protection des données qu'elles assurent.

Les citoyens sont mieux armés et plus conscients de leurs droits : le RGPD renforce la transparence et confère aux particuliers plus de droits, tels que les droits d'accès, de rectification et d'effacement, le droit d'opposition et le droit à la portabilité des données. Aujourd'hui, 69 % de la population de l'UE âgée de plus de 16 ans connaissent l'existence du RGPD tandis qu'ils sont 71 % à avoir entendu parler de leur autorité nationale chargée de la protection des données, selon les résultats d'une enquête de l'Agence des droits fondamentaux de l'Union européenne[2].

Si le bilan de la Commission européenne est globalement positif, il est encore trop tôt pour tirer des conclusions définitives. Toutefois, quelques défis à relever s'annoncent déjà à l'horizon.

En particulier, le traitement des dossiers transfrontaliers basés sur le mécanisme du « guichet unique » requiert une approche encore plus efficace et plus harmonisée ainsi qu'une utilisation effective de tous les outils prévus dans le RGPD, afin que les autorités de protection des données puissent coopérer de manière efficiente.

En ce qui concerne les transferts internationaux des données et à la lumière de l'invalidation du « Privacy Shield », il convient d'adapter les mécanismes de transferts de données, dont les clauses contractuelles types qui sont l'outil de transfert de données le plus couramment utilisé.

Sur le plan des nouvelles technologies telles que l'intelligence artificielle, la blockchain, les objets connectés ou la reconnaissance faciale, la CNPD avec les autres autorités européennes au sein du European Data Protection Board (EDPB), a continué sa veille et ses actions de guidance et d'accompagnement.

[1] https://ec.europa.eu/luxembourg/news/les-r%C3%A8gles-de-lue-en-mati%C3%A8re-de-protection-des-donn%C3%A9es-donnent-aux-citoyens-les-moyens-dagir-et_fr
[2] https://fra.europa.eu/fr/news/2020/dans-quelle-mesure-les-europeens-sont-ils-preoccupes-par-leurs-donnees-caractere-personnel

Le siège de la CNPD à Belval

Ainsi, l'année 2020 fût une année exceptionnelle à beaucoup d'égards. Avec la crise du COVID-19 qui nous accompagnera encore pendant l'année en cours et probablement au-delà, les défis qu'engendrera cette situation en matière de protection de données et de vie privée ne seront pas moindres.

Que ce soit auprès des citoyens, des entreprises privées ou des organismes publics, la CNPD poursuivra son objectif de promouvoir une culture de la protection des données au Luxembourg tout en assurant, dans ce contexte, le rôle de garant du respect du RGPD. Avec les ressources allouées, la CNPD pourra utiliser les moyens juridiques que la législation lui fournit pour garantir au mieux le juste équilibre entre la société de l'information et la protection de la vie privée.

L'autorité de contrôle luxembourgeoise continuera ainsi l'implémentation de son programme de travail 2020-2022 avec une année 2021 certainement marquée par les premières décisions qui ont été prises à l'issue d'enquêtes ouvertes au cours des années précédentes.

Luxembourg, le 31 août 2021

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

UNE ANNÉE EN CHIFFRES

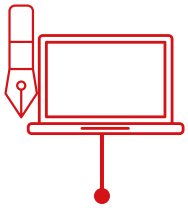
2

SENSIBILISATION, GUIDANCE ET CONSEIL

24

AVIS
contre 16 en 2019

relatifs à des projets ou propositions de loi ou mesures réglementaires, dont notamment des avis sur les lois relatives :
- à la lutte contre la COVID-19 ;
- au système de vidéosurveillance à des fins policières « Visupol » ;
- au registre des fiducies et des trusts.



655

DEMANDES DE RENSEIGNEMENT PAR ÉCRIT
contre 708 en 2019

Les 3 principales catégories de demandes concernent :
1. la pandémie COVID-19 (traçage des personnes, prise de température, télétravail, homeschooling, etc.) ;
2. la surveillance sur le lieu du travail ;
3. le droit des personnes concernées (droit d'accès, droit d'effacement, etc.).

2

NOUVELLES GUIDANCES
contre 3 en 2019

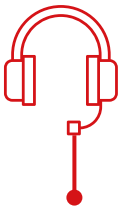
- Le traitement des données personnelles dans le cadre de l'épidémie du coronavirus ;
- Lignes directrices sur les conséquences du Brexit en matière de transferts internationaux de données (mise à jour).

17

FORMATIONS ET CONFÉRENCES
contre 28 en 2019

Nombre d'événements de sensibilisation que la CNPD a organisé ou dans lesquels elle est intervenue comme orateur.

CONFORMITÉ ET CONTRÔLE



485

RÉCLAMATIONS
contre 625 en 2019

Raisons principales :
1. Demande d'effacement ou de rectification non respectée (26 %) ;
2. Non-respect du droit d'accès (23 %) ;
3. Droit d'opposition et prospection (11 %).

379

NOTIFICATIONS DE VIOLATIONS DE DONNÉES
contre 354 en 2019

Cause principale : erreur humaine (65 %)

Nature des incidents :
1. données personnelles envoyées au mauvais destinataire (33 %) ;
2. piratage, hacking (15 %) ;
3. divulgation des données personnelles à la mauvaise personne (12 %).

Plus de la moitié des incidents sont détectés dans les 5 jours de leur survenance.

6

AUDITS OUVERTS

sur le thème de la « transparence » dans le secteur du commerce électronique.

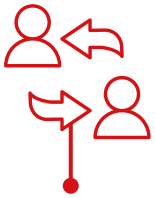
CONFORMITÉ ET CONTRÔLE

33
VISITES SUR PLACE

sur le sujet de la vidéosurveillance et dans le cadre de la campagne thématique « contrôles COVID-19 ».

847
DÉLÉGUÉS À LA PROTECTION DES DONNÉES (DPO)

personnes physiques ou morales déclarées auprès de la CNPD depuis le 25 mai 2018.
dont 116 en 2020



1209
RESPONSABLES DU TRAITEMENT

ont communiqué les coordonnées de leur DPO à la CNPD depuis le 25 mai 2018.
dont 119 en 2020

INTERNATIONAL *EDPB (European Data Protection Board)*

27
RÉUNIONS PLÉNIÈRES

115
RÉUNIONS DES GROUPES DE TRAVAIL

9
NOUVELLES LIGNES DIRECTRICES

6
PROJETS

pour lesquels la CNPD a assumé le rôle de rapporteur.

RESSOURCES HUMAINES

50
COLLABORATEURS
contre 43 en 2019

37,4 ans : moyenne d'âge
4,5 ans : moyenne d'ancienneté auprès de la CNPD

LES ACTIVITÉS EN 2020

3

1 SENSIBILISER LE PUBLIC

L'information des citoyens ainsi que des responsables de traitement et des sous-traitants est une priorité de la CNPD afin de faire connaître les droits et devoirs respectifs de chacun. Elle mène des actions de sensibilisation, informe le public à travers son site Internet et organise ou participe à des formations et conférences.

En raison de la pandémie, la CNPD a organisé et a participé à moins d'événements que les années précédentes. Certaines conférences ont été annulées ou ont été reportées à des dates ultérieures. D'autres ont eu lieu mais en mode virtuel ou quelquefois en mode mixte « à distance / en présentiel ». Certaines initiatives envisagées juste avant le début de la pandémie pour transformer des cours de formation (réalisés jusqu'à présent en présentiel et sur base de slides) en modules virtuels entièrement ou partiellement enregistrés pour être diffusés sur des plateformes d'apprentissage, se poursuivront dans les années à venir.

28 JANVIER 2020 : 14ÈME JOURNÉE INTERNATIONALE DE LA PROTECTION DES DONNÉES

La « Journée Internationale de la protection des données », une initiative du Conseil de l'Europe et de la Commission européenne, est célébrée le 28 janvier de chaque année depuis 2006. 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.

Le 28 janvier 2020, la CNPD a participé au Data Privacy Day organisé par la Fondation Restena et l'Université du Luxembourg.

Le Data Privacy Day est un événement annuel pour les personnes qui s'intéressent à la protection des données et la protection de la vie privée. L'objectif est de sensibiliser et de promouvoir les meilleures pratiques en la matière aux niveaux européen et international.

Monsieur Christophe Buschmann, Commissaire de la CNPD, a tenu le discours d'ouverture et a donné une présentation intitulée « *Feedback on the CNPD governance and process for investigation* ».

ATELIERS DE TRAVAIL « DAPROLAB »

Les « DaProLab » (Data Protection Laboratory) sont des ateliers de travail développés par la CNPD où un seul sujet spécifique défini à l'avance est discuté avec un nombre limité de personnes.

Présentation de Christophe Buschmann lors du Data Privacy Day (28 janvier 2020).

LES ACTIVITÉS EN 2020

3

L'objectif de ces ateliers est l'échange de connaissances, d'idées, d'interprétations et de points de vue sur un sujet prédéterminé entre professionnels de la protection des données.

Les événements de 2018 et 2019 ont notamment porté sur la sécurité des échanges dans le domaine de la santé, les analyses d'impact sur la protection des données ou encore sur les traitements de données dans le secteur des finances/assurances. En raison de la pandémie, les éditions planifiées pour 2020 ont été reportées. Les sujets prévus pour l'année 2020 étaient, entre autres, les analyses d'impact sur la protection des données (AIPD) dans le contexte des recherches scientifiques et l'identification des (co-)responsables de traitement et sous-traitants dans le contexte des recherches scientifiques.

FORMATIONS, CONFÉRENCES ET SÉMINAIRES

La Commission nationale a aussi participé à des formations, conférences et séminaires pour sensibiliser des publics plus experts aux enjeux de la protection des données.

Comme les années précédentes, l'autorité de contrôle est intervenue lors de cours de formation générale sur la protection des données auprès de l'EST (Ecole Supérieure de Travail), de l'INAP (Institut national d'administration publique) de la CSSF (Commission de Surveillance du Secteur Financier) et de la CSL (Chambre des Salariés) / LLLC (Luxembourg Life Long Learning Center).

Les séances de formations et de conférences animées par la CNPD au cours de l'année ont été :

- *« Cyberprotection ou comment appliquer correctement le RGPD en médecine générale? »* lors de la conférence « Health 4.0 » organisée par l'Association Luxembourgeoise pour la Formation Médicale Continue ;
- *« Le RGPD au cœur de la relation-client - quelles règles à respecter? »* organisé par la Chambre des Métiers ;
- *« Le règlement général sur la protection des données: comment le mettre en place dans mon bureau de courtage? »* organisé par l'APCAL (Association Professionnelle des Courtiers en Assurances au Luxembourg) ;
- *« GDPR Evaluation after 2 years »* organisé par l'ISACA (Association international de l'audit et du conseil informatique) ;
- *« Le bilan de deux années de RGPD »* organisé par la représentation de la Commission européenne au Luxembourg dans le cadre de ses « Midis du consommateur européen » ;
- *« Le contrôle de la conformité : l'approche de la CNPD »*, organisé par l'INHESJ (Institut National des Hautes Etudes de la Sécurité et de la Justice, France) ;
- *« How can GDPR certification support cross-border data transfers? »* lors d'un panel de la conférence « Digital Around the World » intitulé « Making Data Protection by Design a Reality - Towards a Global Convergence » la conférence « Digital Around the World »;
- *« Updates from the CNPD »* lors du *PwC Cybersecurity Day ;*

- Table ronde « Bilan RGPD - 2 ans après » workshop *« Continuité des affaires en période de COVID-19: quels défis pour la protection des données personnelles? »* lors des Cybersecurity & Data Protection Days 2020 organisés par la Chambre de Commerce du Luxembourg et son Enterprise Europe Network, en collaboration avec SECURITYMADEIN.LU et MGSI ;
- *« La CNPD et les autorités de contrôle sous le RGPD »* organisé par Chambre des Salariés dans le cadre du cours du soir « Le professionnel en protection des données personnelles » ,
- *« GDPR and other regulatory considerations in Europe »* organisé par l'accélérateur Foundry de l'entreprise Mason Bower pour le compte d'une sélection de startups souhaitant s'implanter au Luxembourg.

Depuis 2020, la CNPD est associée au développement d'un nouveau programme de formation dans le domaine de la cybersécurité de l'enseignement professionnel supérieur niveau BTS, proposé par le Lycée Guillaume Kroll à Esch-sur-Alzette. La CNPD a contribué à la définition du programme pour ce qui est des aspects de protection des données personnelles. Les cours démarreront dès la rentrée scolaire en automne 2021, suite à l'obtention en juin 2021 de l'accréditation du BTS par le Ministère de l'Enseignement Supérieur et de la Recherche.

VEILLE TECHNOLOGIQUE ET JURIDIQUE

La CNPD a commencé à mettre en place début 2020 une unité de veille technologique et de veille juridique et réglementaire. Celle-ci doit permettre aux services de la CNPD :

- d'avoir un aperçu rapide et sommaire sur la problématique des données personnelles dans le contexte des nouvelles technologies ; et
- de pouvoir ainsi orienter leurs recherches dans le contexte du traitement de réclamations ou d'enquêtes et pour la rédaction d'avis juridiques ou la préparation de formations de guidances ou de recommandations.

Les experts de la CNPD ont ainsi ouvert ou mis à jour les dossiers suivants au cours de l'année 2020 :

- Fintech
- COVID-19 tracing Apps
- Télétravail
- Homeschooling
- Intelligence artificielle

COLLABORATIONS AVEC LES ACTEURS DE LA RECHERCHE ET DE L'INNOVATION (RDI)

La politique gouvernementale met un accent important sur la diversification économique du pays par la recherche et l'innovation (RDI). Les priorités des acteurs RDI publics et privés sont largement orientées vers les sciences

numériques, la cybersécurité, l'intelligence artificielle, la confiance numérique et, en général, les technologies digitales innovantes.

Dans ce contexte, la CNPD se doit d'observer activement les grandes orientations politiques, les projets d'envergure des acteurs nationaux et de rester ouverte à des collaborations jugées utiles et nécessaires pour le développement de produits et services respectueux de la protection des données à caractère personnel et de la vie privée.

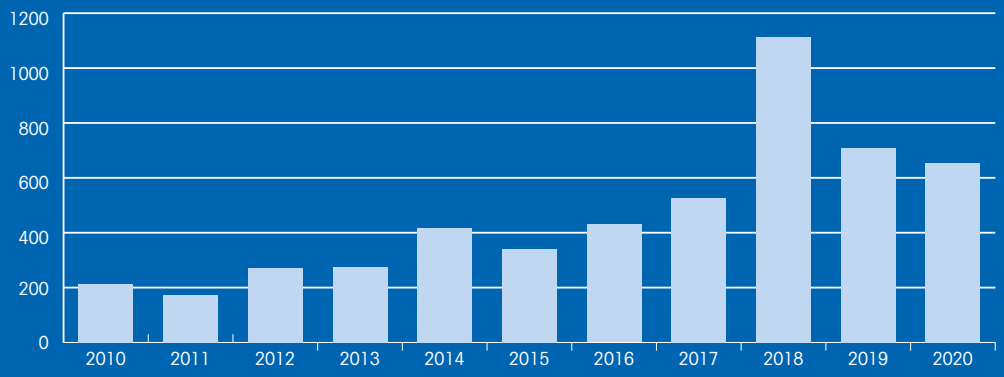
La CNPD a été sollicitée pour participer aux projets suivants en faisant parti du comité de suivi ou du comité de pilotage du projet :

- *National Digital Twin :* projet du LIST (Luxembourg Institute of Science and Technology) et cofinancé par le FNR ;
- *Smart Schoul 2025 :* projet FNR de l'Interdisciplinary Center for Security, Reliability and Trust (SnT) de l'Université du Luxembourg en collaboration avec le SCRIPT du Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse, et le Lycée Edward Steichen Clervaux (LESC).

Dans le contexte des activités de la « Research Luxembourg COVID-19 Taskforce » la CNPD a contribué aux travaux d'évaluation et de préparation pour la mise en place d'une solution nationale d'une Contact Tracing App.

Une participation active à ces projets permet à la CNPD de rappeler aux acteurs de la recherche publique et de l'innovation les principes importants de la protection des données à caractère personnel comme notamment le « Privacy by design and by default », la limitation des durées de conservation, la limitation des finalités des traitements, la détermination des conditions de licéité ou la clarification des liens entre responsables du traitement et sous-traitants.

ÉVOLUTION DU NOMBRE DE DEMANDES D'INFORMATION PAR ÉCRIT



2 RÉPONDRE AUX DEMANDES D'INFORMATION DE PARTICULIERS ET DE PROFESSIONNELS

La CNPD informe et conseille les particuliers et les professionnels qui souhaitent obtenir des renseignements juridiques, des informations sur l'exercice de leurs droits ou une assistance à la mise en conformité de leurs traitements à la législation relative à la protection des données. Un service dédié répond aux questions des requérants reçues par courriel, téléphone ou courrier postal.

La Commission nationale a reçu 655 demandes d'information par écrit en 2020, soit une diminution par rapport à l'année précédente (-7 %). Toutefois, nous observons une augmentation progressive depuis 2011, marquée par le pic exceptionnel en 2018, année d'entrée en application du RGPD.

En 2020, un peu moins que la moitié des demandes provenaient directement de personnes concernées, en nette progression en comparaison à l'année 2019. Les entreprises privées introduisent toujours de nombreuses demandes, tout comme les administrations publiques. La Commission nationale a été sollicitée par un certain nombre d'entités publiques, dont de plus en plus d'administrations communales.

Sans surprise, l'année 2020 a été marquée par de nombreuses sollicitations portant sur les traitements de données en lien avec la pandémie COVID-19, en particulier en matière de traçage des personnes exposées à une personne testée positivement, à la prise de température et à l'utilisation de plateformes numériques pour la réalisation de visioconférences. La surveillance sur le lieu du travail, avant tout au moyen des nouveaux outils informatiques mis en place par l'employeur, a été un sujet de préoccupation avec le recours massif au télétravail tout au long de l'année 2020.

LES ACTIVITÉS EN 2020

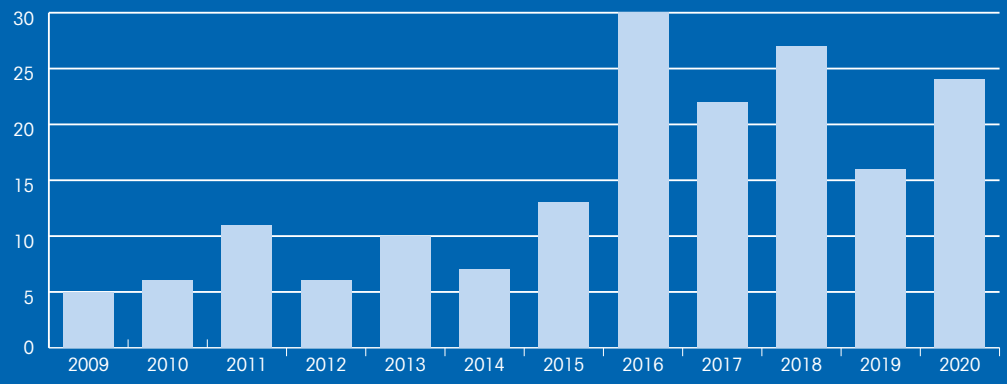
3

Comme les années précédentes, un grand nombre de demandes visaient l'exercice des droits des personnes concernées, en particulier le droit d'accès aux données à caractère personnel et le droit à l'effacement. Ces demandes démontrent que les citoyens utilisent davantage les droits consentis par le RGPD et que la protection des données continue d'être un sujet de préoccupation majeure.

D'autres questions récurrentes concernent notamment :

- les conditions de licéité (notamment le consentement) ;
- l'éducation (surtout le droit à l'image) ;
- la géolocalisation ;
- les ressources humaines ;
- la surveillance (sur le lieu de travail) ;
- l'utilisation de la pièce d'identité / matricule (RNPP) ;
- la vidéosurveillance.

ÉVOLUTION DU NOMBRE DES AVIS



3 INTERVENIR DANS LE PROCESSUS LÉGISLATIF

La CNPD conseille la Chambre des députés, le Gouvernement et d'autres institutions et organismes publics à travers les avis relatifs aux projets de loi et aux mesures réglementaires ou administratives concernant le traitement de données personnelles et présentant un risque particulier au regard de la vie privée des personnes concernées.

En 2020, la Commission nationale a émis 24 avis sur des projets de loi ou de règlements grand-ducaux, soit 8 de plus qu'en 2019.

Tous les avis peuvent être consultés sur le site Internet de la CNPD à l'adresse https://cnpd.public.lu/fr/publications/rapports/index.html.

Les thématiques suivantes ont été abordées dans les avis de la CNPD :

- la lutte contre le COVID-19 (8 avis) ;
- la lutte contre le blanchiment de capitaux et contre le financement du terrorisme (3 avis) ;
- le traitement des données à caractère personnel dans le secteur des communications électroniques ;
- le traitement de données concernant la santé en matière d'assurance et de réassurance ;
- l'examen-concours pour l'admission au stage de la Police ;
- la qualité des services pour personnes âgées ;
- le bail à usage d'habitation ;
- les modalités d'enregistrement des établissements des exploitants du secteur alimentaire ;
- les dossiers d'aides relatives au logement ;
- la reconnaissance des qualifications professionnelles dans le domaine de la navigation intérieure.

LES ACTIVITÉS EN 2020

3

Par ailleurs un avis en matière de surveillance sur le lieu du travail, ci-après désigné « avis travail » a été adopté en 2020 (procédure de l'article L.261-1 paragraphe (4) du Code du travail) sur la géolocalisation des voitures de service et des engins de chantier.

Finalement, la CNPD a également rendu 4 avis relatifs aux traitements de données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale. Ceux-ci sont présentés dans la partie II.9.b) dédiée spécifiquement au rôle de la Commission nationale portant sur le contrôle des traitements de données opérés par les autorités répressives ou les autorités de sécurité nationale.

Parmi les avis rendus en 2020, la CNPD voudrait mettre en avant les trois avis suivants. Les autres avis peuvent être consultés sur le site de la CNPD à l'adresse https://cnpd.public.lu/fr/decisions-avis.html.

AVIS RELATIFS À LA LUTTE CONTRE LE COVID-19

En 2020, la Commission nationale a émis 8 avis concernant l'introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre le COVID-19.

La Commission nationale a souligné dans ses avis que la protection des données personnelles n'était pas à considérer comme obstacle à la mise en place d'un traitement de données à caractère personnel dans le cadre de la lutte contre l'épidémie COVID-19, tant que les principes fondamentaux prévus par le RGPD sont respectés. Elle 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.

Dans ses prises de position, la CNPD a notamment commenté :

- la création d'un système d'information par la Direction de la santé, afin de surveiller l'évolution de la situation liée au COVID-19 et le traitement de données « sensibles », à travers ce système ;
- la mise en place d'un système de traçage pour identifier le plus tôt possible toute personne à risque ou à haut risque d'être infectée afin de mettre en œuvre les précautions nécessaires (comme une mise en quarantaine) et de prévenir ainsi la dissémination de l'infection par ces personnes à leur tour contagieuses ;
- la durée de conservation des données à caractère personnel figurant dans le système d'information et l'anonymisation/pseudonymisation de ces données ;
- les personnes autorisées dans le cadre du traçage des contacts d'accéder aux données des personnes infectées ou à haut risque d'être infectées contenues dans le système d'information ;
- la collecte des données à caractère personnel dans le cadre du programme de vaccination. Elle a pris position quant aux questions concernant la finalité poursuivie par la collecte des données et la durée de conservation des données collectées dans le cadre du programme de vaccination.

La CNPD s'est par ailleurs autosaisie pour aviser le projet de loi n°7635 qui prévoit que *« les salariés doivent signaler immédiatement, à l'employeur ou aux salariés désignés et aux délégués à la sécurité et à la santé, toute situation de travail dont ils ont un motif raisonnable de penser qu'elle présente un danger grave et immédiat pour la sécurité et la santé dans le cadre de l'épidémie de COVID-19) ».*

L'auto-saisine de la CNPD est intervenue dans le cadre de nombreuses demandes d'information et de réclamations introduites auprès d'elle concernant d'une part les données, notamment de santé, que les salariés seraient autorisés à communiquer à l'employeur en cas de suspicion ou de contamination au virus SARS-CoV-2, et d'autres part les obligations de l'employeur quant au traitement de ces données.

AVIS SUR LE REGISTRE DES FIDUCIES ET DES TRUSTS

La CNPD a rendu un avis sur le projet de loi n°7216B, qui vise à transposer l'article 31 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 en tenant compte de la recommandation 25 du GAFI.

Le projet de loi comporte deux volets. Premièrement, le projet de loi prévoit l'obligation pour les fiduciaires et les trustees d'obtenir et de conserver des données relatives aux bénéficiaires effectifs ainsi qu'à d'autres personnes spécifiées dans le projet de loi. Deuxièmement, le texte vise à instaurer un registre des fiducies et des trusts tenu par l'Administration de l'enregistrement, des domaines et de la TVA dans lequel les fiduciaires et les trustees devront faire inscrire certaines données qu'ils sont obligés de collecter en vertu de la loi en projet.

La Commission nationale a formulé des observations sur plusieurs éléments du projet de loi. Elle a notamment rappelé la nécessité de respecter le principe de minimisation de données et a ainsi recommandé de prévoir avec

précision les données devant être collectées par les trustees et les fiduciaires dans le cadre de leurs obligations découlant du présent projet de loi. Conformément au principe de minimisation de données, seules les données nécessaires devraient être traitées.

Par ailleurs, quant à l'accès au registre, la CNPD a notamment préconisé de limiter l'accès des professionnels aux données contenues dans le registre aux seules données nécessaires. En ce qui concerne l'accès par le grand public sur base de l'intérêt légitime, la CNPD a rappelé l'importance d'une définition claire de l'intérêt légitime et a estimé nécessaire de définir les critères sur base desquels cet intérêt légitime serait analysé. Elle a également formulé des observations quant aux données à caractère personnel devant être fournies avec la demande pour accéder au registre.

La Commission nationale a par ailleurs émis des recommandations relatives aux traitements des autorités nationales et des organismes d'autorégulation, notamment en ce qui concerne le respect du principe de limitation des finalités et le transfert de données vers des pays tiers.

PRÉVENTION DE L'UTILISATION DU SYSTÈME FINANCIER AUX FINS DU BLANCHIMENT DE CAPITAUX OU DU FINANCEMENT DU TERRORISME

La CNPD a rendu son avis sur le projet de loi n°7467, qui vise à transposer certaines dispositions de la directive 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 et à mettre en œuvre des recommandations du GAFI, notamment dans le cas où ces recommandations ne font pas l'objet de dispositions équivalentes dans la directive (UE) 2015/849. Elle a formulé des observations sur plusieurs éléments du projet de loi.

Dans son avis, la CNPD a tout d'abord rappelé l'importance de respecter la législation en matière de protection de la vie privée et des données à caractère personnel lors de la transposition de la directive 2018/843 et de la mise en œuvre des recommandations du GAFI.

Elle a également émis des remarques relatives à la durée de conservation des données par les professionnels ainsi qu'aux droits des personnes concernées, soulevant la nécessité de prévoir un cadre légal précis et proportionnel au but recherché. En ce qui concerne les droits des personnes concernées, la CNPD a recommandé de préciser les cas dans lesquels le droit d'accès des personnes concernées pourrait être limité et de prévoir un droit d'accès indirect en cas de limitation de ce droit.

La Commission nationale a finalement fait des suggestions quant aux traitements de la CRF, des autorités nationales et des organismes d'autorégulation, notamment en ce qui concerne le respect du principe de limitation des finalités et le transfert de données vers des pays tiers.

4 GUIDER LES ACTEURS PRIVÉS ET PUBLICS

Les acteurs des secteurs privé et public doivent adopter une conduite préventive et responsable à l'égard des données à caractère personnel qu'ils collectent. Les guider et les orienter dans cette démarche est un des rôles de l'autorité de contrôle. Ce rôle est assumé par la CNPD en élaborant des recommandations ou des guidances sur des thématiques pour un public cible bien spécifiques.

COLLECTE DE DONNÉES PERSONNELLES DANS LE CONTEXTE DU CORONAVIRUS (COVID-19)

Les données à caractère personnel, notamment de santé, sont au cœur des problématiques liées à la crise sanitaire du COVID-19. Dès le début de la pandémie, la CNPD a accompagné les acteurs privés et publics luxembourgeois.

Ceux-ci ont été confrontés à des défis complexes dans leur fonctionnement quotidien. De nouveaux défis ont surgi au fur et à mesure du confinement, puis du déconfinement, notamment en raison du retour des salariés sur leur lieu de travail ainsi que lors des étapes successives en fonction des mesures sanitaires prises par le gouvernement.

Les professionnels et les particuliers se sont interrogés tant sur les mesures mises en œuvre pour limiter la propagation du virus et assurer en toute sécurité la reprise de l'activité, que sur les conditions dans lesquelles les données personnelles, notamment de santé, peuvent être utilisées.

La CNPD a publié des recommandations pour orienter les professionnels dans la poursuite de leurs activités et pour répondre aux questions des personnes sur leurs droits.

Dans sa guidance, la CNPD a notamment rappelé quelques règles concernant :

- l'obligation de sécurité des employeurs ;
- l'obligation de sécurité des salariés/agents ;
- le traitement des données par les employeurs :
  - les relevés de température à l'entrée des locaux ;
  - la réalisation de tests par l'employeur et de questionnaires sur l'état de santé ;
- les demandes et recommandations des autorités sanitaires.

Les recommandations ont été mises à jour sur le site Internet de la CNPD[3] à plusieurs reprises en tenant compte de l'évolution de la pandémie.

LIGNES DIRECTRICES SUR LES CONSÉQUENCES DU BREXIT EN MATIÈRE DE TRANSFERTS INTERNATIONAUX DE DONNÉES

Suite à l'accord entre le Royaume-Uni et la Commission européenne, publié le 25 décembre 2020, la CNPD a mis à jour ses lignes directrices concernant les conséquences du Brexit en matière de transferts internationaux de données. Ces lignes directrices sont destinées à guider les entreprises, organismes publics et associations luxembourgeoises qui sont amenés à transférer des données à caractère personnel vers le Royaume-Uni, et qui entendraient poursuivre de tels transferts en 2021.

La Commission nationale a également mis à jour son dossier thématique consacré aux transferts internationaux de données à caractère personnel par rapport au règlement général sur la protection des données.

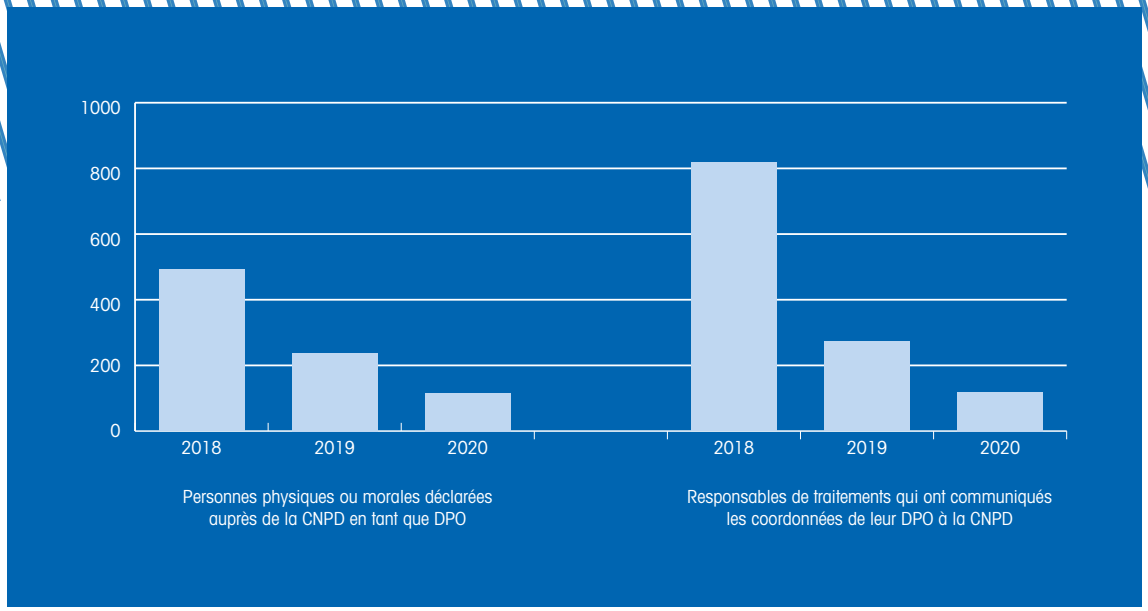
Les cas de figure suivants sont traités dans le dossier thématique :

- Transferts au sein de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande) ;
- Transferts vers un pays en dehors de l'Espace économique européen disposant d'un niveau de protection adéquat ;
- Transferts vers un pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat ;
- La coopération internationale en matière policière et judiciaire ;
- Les conséquences du Brexit en matière de transferts internationaux de données.

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, ou DPO de l'anglais « Data Protection Officer ») qu'ils ont, le cas échéant, désigné.

[3] https://cnpd.public.lu/fr/actualites/national/2020/03/coronavirus.html



En 2020, 119 responsables du traitement ont communiqué les coordonnées de leur DPD à la Commission nationale. Depuis le 25 mai 2018, 1209 responsables du traitement ont effectué cette démarche.

Au total, 847 personnes physiques ou morales ont été déclarées auprès de la CNPD, dont 116 en 2020.

Pour faciliter la communication de ces informations, la CNPD a mis en ligne un formulaire, ainsi qu'un espace dédié sur son site qui répond aux questions fréquemment posées.

A titre de rappel, la désignation d'un DPD est obligatoire dans trois situations :

- 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 ;
- 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 est évident qu'un organisme n'est pas tenu de désigner un DPD, la CNPD recommande de toujours documenter l'analyse interne effectuée afin de déterminer si, oui ou non, il y a lieu de désigner un DPD.

LES ACTIVITÉS EN 2020

3

5 ACCOMPAGNER LA MISE EN CONFORMITÉ

Le règlement général sur la protection des données a introduit plusieurs outils d'application volontaire pour permettre aux organismes de gérer leur conformité et de démontrer qu'ils respectent la législation: analyses d'impact sur la protection des données, certifications, codes de conduite ou encadrement des transferts internationaux de données.

CERTIFICATION

La CNPD a continué ses travaux démarrés dès 2018 pour mettre en place et gérer les activités liées à la certification tel que proposé dans le RGPD. Ces instruments permettent aux responsables du traitement et sous-traitants de démontrer que leurs opérations de traitement respectent le règlement.

La mise en place de mécanismes de certification peut favoriser la transparence et le respect du RGPD et permettre aux personnes concernées d'évaluer le niveau de protection des données offert par les produits, services, processus ou systèmes des acteurs privés et publics.

Le cadre d'application pratique de ces nouveaux outils est développé en concertation avec les autres autorités de contrôle au niveau de l'EDPB pour assurer une cohérence mais également, au niveau national, en collaboration avec les acteurs intéressés du secteur privé.

Les nombreux échanges entre la CNPD et les entreprises pendant la phase de préparation au RGPD, ont démontré que celles-ci ont un intérêt particulier pour la certification selon le règlement.

Etant persuadée de la valeur ajoutée que la certification peut offrir, la CNPD a pris une approche particulièrement proactive en développant, conjointement avec les entreprises d'audit, un référentiel de certification basé sur le cadre d'évaluation international de conformité ISAE *(International Standard on Assurance Engagements)*.

Ainsi, la CNPD a proposé le schéma dénommé **« GDPR-CARPA »** qui a été soumis à une première consultation publique en juin 2018. Après avoir intégré jusque fin 2020 les retours reçus au niveau national et européen, en particulier via les échanges avec les autres autorités de contrôle européennes au sein du EDPB, une consultation finale a été réalisée début 2021.

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 ;

- Le deuxième pilier concerne les **critères d'agrément** auxquels doit répondre une organisation qui souhaite agir en tant qu'organisme de certification.

Dans ce contexte, elle a contribué en tant que lead-rapporteur au Comité européen pour la Protection des Données à :

- la mise en place de procédures pour l'adoption des critères d'agrément des organismes de certification ;
- l'adoption des critères de certification et
- l'adoption d'un label européen pour la certification.

Il est à noter que la CNPD est la première autorité de protection des données en Europe à soumettre ses critères d'agrément à l'EDPB pour avis et, une fois ces critères adoptés, le Luxembourg sera le premier pays à permettre la certification selon les critères du RGPD.

Approbation des critères d'agrément des organismes de certification

Le 3 avril 2020, la CNPD a adopté la décision n°8/2020 portant approbation des critères d'agrément des organismes de certification.

Ces critères d'agrément s'appliquent aux organismes de certification dont les activités portent sur des mécanismes et critères de certification que la CNPD a désigné par le label « set Alpha » tel que défini dans le document annexé à la décision.

L'agrément a pour objectif d'attester avec l'autorité nécessaire les compétences des organismes de certification, ce qui permet d'instaurer la confiance dans le mécanisme de certification.

LES ACTIVITÉS EN 2020

3

CODES DE CONDUITE

Les codes de conduite sont des outils de responsabilisation volontaires qui définissent des règles spécifiques en matière de protection des données pour certaines catégories de responsables du traitement et de sous-traitants.

Ils peuvent constituer un outil de responsabilisation utile et efficace en fournissant une description détaillée de l'ensemble des comportements les plus appropriés les plus éthiques et reprenant les meilleures pratiques dans un secteur donné.

Les associations professionnelles ou organismes représentants un secteur donné peuvent élaborer des codes pour aider les entreprises de ce secteur à respecter le RGPD de façon efficace.

En 2020, la CNPD était en contact avec la fédération d'un secteur professionnel qui a entamé une approche de mise en place d'un code de conduite. Cependant la CNPD constate que, contrairement aux pays voisins, les acteurs au Luxembourg n'ont pas encore vraiment démontré leur intérêt pour des codes de conduite. Toutefois, elle les encourage à le faire et envisage de promouvoir l'utilisation de cet outil dans un futur proche.

ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

AIPD - de quoi s'agit-il ?

Une AIPD (Analyse d'impact sur la protection des données, ou DPIA de l'anglais *« Data Protection Impact Assessment »*) est un outil qui aide à identifier et à minimiser les risques de protection des données de nouveaux projets comportant des processus de traitement de données à caractère personnel. Elle fait partie des obligations prévues par le RGPD pour les responsables du traitement et contribue fortement à l'approche de responsabilisation prônée par le RGPD, en particulier via les concepts de la protection des données dès la conception et protection des données par défaut (*« Privacy by design », « Privacy by default »*).

Une AIPD aide les responsables de traitement à identifier et à traiter les problèmes à un stade précoce, à démontrer leur conformité avec les obligations en matière de protection des données et à répondre aux attentes des individus en matière de vie privée.

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 AIPD.

La CNPD a élaboré une liste de types d'opérations de traitements pour lesquels elle estime qu'une AIPD est obligatoire dans tous les cas[4].

[4] La liste peut être consultée sur le site Internet de la CNPD : https://cnpd.public.lu/fr/professionnels/obligations/AIPD.html

GDPR COMPLIANCE SUPPORT TOOL

Afin d'aider les organisations dans leurs efforts de mise en conformité, la CNPD a développé dès 2017 avec des partenaires externes (Luxembourg Institute of Science and Technology, LIST, la société eProseed et avec le soutien de Digital Lëtzebuerg) un outil en ligne leur permettant d'autoévaluer leur niveau de maturité en matière de protection des données : le *« GDPR Compliance Support Tool »* (CST).

Cet outil a connu un intérêt continu avec environ 2000 organisations enregistrées comme utilisateur au 31.12.2020.

L'outil a rempli son rôle d'assistance à la mise en conformité RGPD aux organisations pour l'entrée en vigueur du règlement en 2018 et il n'est à ce jour plus adapté à l'évolution de la matière.

Il a été mis hors ligne en septembre 2021. La CNPD a entamé des réflexions pour proposer de nouveaux outils.

Si, suite à cette analyse de risques, il en résulte que le niveau de risque résiduel reste élevé, l'organisme doit obligatoirement consulter la CNPD qui va donner un avis sur le traitement envisagé et les risques y liés.

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 2020, deux demandes d'avis préalables ont été soumises à la CNPD. Ce chiffre très peu élevé en comparaison avec ceux des pays limitrophes indique que l'utilisation des analyses d'impact ne semble pas encore être très répandue parmi les responsables du traitement établis au Luxembourg.

LES ACTIVITÉS EN 2020

3

TRANSFERTS INTERNATIONAUX DE DONNÉES PERSONNELLES

Les données à caractère personnel peuvent circuler librement depuis le Luxembourg au sein de l'Espace économique européen (EEE), tant que les principes généraux du RGPD sont respectés. Les transferts de données hors de l'UE et de l'EEE sont possibles, à condition d'assurer un niveau de protection des données suffisant et approprié. Ces transferts doivent être encadrés en utilisant différents outils juridiques (clauses contractuelles, règles d'entreprise contraignantes (BCR), codes de conduite, mécanismes de certification ou garanties spécifiques pour le transfert entre autorités ou organismes publics).

Invalidation du « Privacy Shield »

Le 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE) a invalidé la décision 2016/1250 sur l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (*« Privacy Shield »*). Dans son arrêt dans l'affaire Data Protection Commissioner contre Facebook Ireland et Maximilian Schrems (Schrems II), la Cour a constaté que le *« Privacy Shield »* n'assurait pas un niveau de protection essentiellement équivalent à celui garanti par le RGPD et la Charte des droits fondamentaux de l'UE.

Par conséquent, les entreprises ne peuvent plus légitimer leurs transferts vers les États-Unis d'Amérique sur base du EU-US *« Privacy Shield »* Framework, mais devront réaliser la même analyse que pour tout autre pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat.

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 groupes 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.

En 2020, la CNPD a traité des dossiers concernant les règles d'entreprise contraignantes (BCRs, article 47 du RGPD) dont 7 en qualité d'autorité principale (c'est-à-dire pour des entreprises multinationales dont l'établissement principal dans l'Union européenne est situé au Luxembourg), 3 en qualité d'autorité secondaire (*« co-reviewer »*) (c'est-à-dire en appui de l'autorité de contrôle principale) et 15 en qualité d'autorité concernée.

LES ACTIVITÉS EN 2020

3

6 TRAITER LES RÉCLAMATIONS DES CITOYENS

Si une réclamation directe d'une personne concernée auprès d'un responsable du traitement est restée sans suite, celui-ci peut s'adresser à la CNPD. Le traitement des réclamations émanant des personnes concernées compte parmi ses missions. La CNPD informe en principe le responsable du traitement des faits soulevés dans la réclamation et, en cas de manquements constatés, lui demande de se mettre en conformité et de respecter les droits des personnes concernées.

ADOPTION DE LA PROCÉDURE RELATIVE AUX RÉCLAMATIONS

Le 16 octobre 2020, la CNPD a adopté sa procédure relative aux réclamations[5].

La CNPD examine ainsi en premier lieu si une réclamation est justifiée, c'est-à-dire qu'elle vérifie si les faits allégués par le réclamant relatifs à un traitement de données à caractère personnel sont susceptibles de constituer ou non une violation de la législation applicable en matière de protection des données.

Lorsque la CNPD estime que le traitement de données litigieux est effectivement contraire à la législation, elle s'efforcera d'y remédier, dans une première étape, sans avoir à déclencher une procédure d'enquête formelle conformément aux articles 37 à 41 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.

Elle a ainsi un pouvoir discrétionnaire pour apprécier si elle instruit une réclamation ou non. En fonction des caractéristiques propres à chaque réclamation, la CNPD peut décider d'instruire ou de ne pas instruire une réclamation en tenant compte notamment du degré de gravité des faits allégués, de la violation alléguée, du degré d'impact sur les droits et libertés fondamentaux, du degré de priorité par rapport au nombre de réclamations et des ressources disponibles.

RÉCLAMATIONS NATIONALES ET EUROPÉENNES

En 2020, la CNPD a reçu un total de 485 réclamations :

- 324 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 ;
- Aux réclamations traitées au niveau national, s'ajoutent à travers le système européen de coopération, 161 réclamations pour lesquelles la CNPD a été l'autorité chef de file présumée du fait que le responsable du traitement ayant des activités au niveau européen, avait établi son siège au Luxembourg. Ces réclamations sont portées à l'attention de la CNPD par l'autorité ou les autorités de contrôle des pays dans lesquels le ou les personnes concernées ont déposé leur plainte via le système IMI.

Par rapport à l'année précédente, il s'agit d'une diminution de 140 réclamations. Toutefois, leur nombre reste très élevé depuis l'entrée en application du RGPD avec une moyenne de 520 réclamations par année depuis 2018.

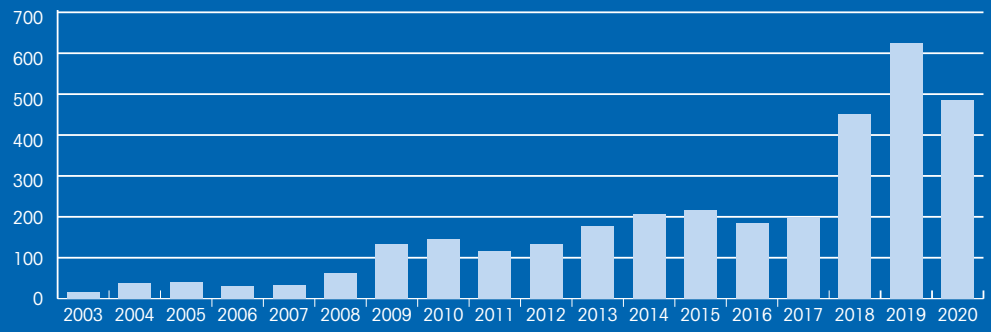
Les **demandes d'effacement ou de rectification** de données constituent 26 % des réclamations reçues en 2020. Il s'agissait, entre autres, de demandes de fermeture de comptes auprès de services/commerces en ligne ou de

[5] https://cnpd.public.lu/content/dam/cnpd/reglements-cnpd/CNPD-Procedure-Reclamationsversdef20201016.pdf

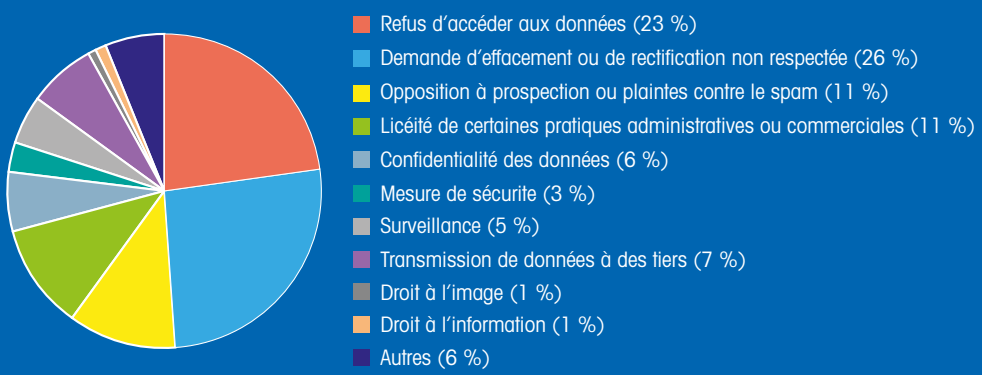
LES ACTIVITÉS EN 2020

3

ÉVOLUTION DU NOMBRE DE RÉCLAMATIONS



MOTIFS DES RÉCLAMATIONS



LE SYSTÈME D'INFORMATION DU MARCHÉ INTÉRIEUR (IMI)

Le système IMI est la plateforme informatique de l'Union européenne qui garantit la bonne mise en œuvre de la coopération entre les autorités de contrôle pour une large panoplie de réglementations. Cet outil a également été mis au service du RGPD depuis le 25 mai 2018 tel que prévu par le RGPD. Les autorités de contrôle des États membres coopèrent étroitement pour assurer une protection uniforme des droits des personnes en matière de protection des données dans l'ensemble de l'UE.

Aujourd'hui plus que jamais, l'assistance mutuelle et la coordination de la prise de décision dans les affaires transfrontalières 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 transfrontalière.

A l'aide du système IMI, les autorités de contrôle peuvent 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 ;
- consulter le Comité européen de la protection des données pour obtenir un avis ou une décision contraignante.

demandes d'effacement de données personnelles (adresses e-mail, évaluations, etc.) accessibles sur des sites Internet (comme des annuaires par exemple).

Presque un quart des réclamations (23 %) a été motivé par le **non-respect du droit d'accès** par les responsables du traitement. Dans certains cas, ces derniers ont refusé aux personnes concernées 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.

11 % des plaintes étaient relatives au **droit d'opposition**, notamment dans le domaine de la prospection. La CNPD est intervenue lorsque des liens de désabonnement à prospection dans des courriels n'étaient pas fonctionnels ou lorsque le responsable du traitement ne donnait pas suite aux demandes d'opposition.

Dans 11 % des cas, les réclamants ont demandé à la CNPD de **vérifier la licéité de certaines pratiques administratives ou commerciales**. Ils ont notamment remis en cause :

- la collecte illicite ou excessive de données (p.ex. de plaques d'immatriculation) ;
- 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) ;
- des dispositions relatives à la protection des données mentionnées dans des conditions générales relatives à des commerces ou des services en ligne ;
- la durée de conservation des données collectées ;
- la licéité de traitement des dossiers du personnel ;
- la création d'annuaires sans le consentement des personnes concernées ;
- des décisions individuelles automatisées.

La **transmission non autorisée de données à des tiers** a également conduit à un certain nombre de réclamations (7 %). 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 ;
- 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 ») ;
- des consultations non autorisées dans le registre national des personnes physiques RNPP) par des agents du secteur public.

La majorité des requêtes liées à la **surveillance sur le lieu du travail** (5 % des réclamations) concernaient la vidéosurveillance.

DEMANDES DE MISE EN CONFORMITÉ

En 2020, 167 réclamations nationales ont conduit à l'adoption de mesures de mise en conformité. Il s'agit des cas où la CNPD a demandé au responsable du traitement de mettre en place des mesures pour se conformer au RGPD (ex. faire droit à une demande d'accès, d'effacement, d'opposition, modification des notices d'informations afin de se conformer aux exigences des articles 13 et 14 du RGPD, mise en place de mesures de sécurité supplémentaires, etc.) sans avoir dû déclencher une procédure d'enquête formelle conformément aux articles 37 à 41 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 .

En plus des réclamations introduites au niveau national, s'ajoutent à travers le système européen de coopération encore 65 réclamations qui ont été clôturées par des demandes de mise en conformité.

7 ANALYSER LES 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.

VIOLATIONS DE DONNÉES DANS LE CADRE DU RGPD

Le RGPD exige qu'une violation de sécurité entraînant, de manière accidentelle ou illicite, la **destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel** doit être gérée dans le respect des exigences des articles 33 et 34 du RGPD.

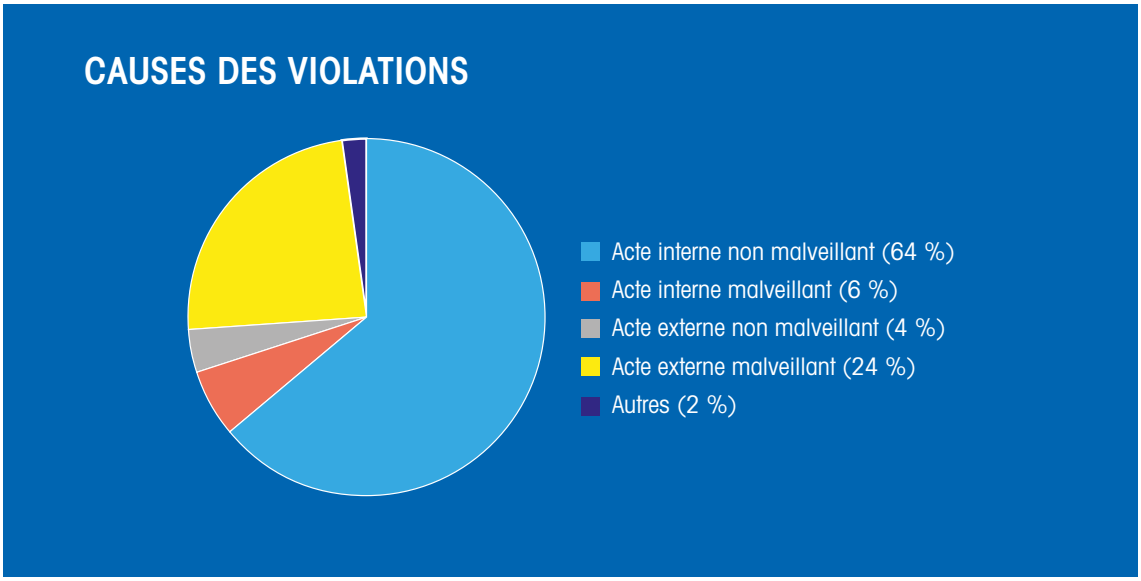
Les responsables du traitement doivent notifier les violations de données à caractère personnel à la CNPD dans un délai de 72 heures après en avoir pris connaissance si la violation en question est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

La CNPD tient à préciser que les statistiques suivantes sont uniquement 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 qui se produisent dans les organisations. La CNPD ne connaît pas le chiffre total des incidents qu'il est difficile d'estimer. Toutefois, les responsables du traitement sont tenus de maintenir une documentation de tous les incidents de sécurité impliquant des données à caractère personnel.

En 2020, 379 violations de données ont été notifiées à la CNPD, soit 25 de plus qu'en 2019.

LES ACTIVITÉS EN 2020

3



Au total, depuis l'entrée en application du RGPD le 25 mai 2018, la Commission nationale a reçu 905 violations de données. Cela correspond à une moyenne de 29 notifications de violations de données par mois.

La principale cause de violation de données à caractère personnel reste **l'erreur humaine** (acte interne non malveillant) dans 64 % des cas.

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 conséquences 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 probablement permis d'éviter ce type d'incident.

Des **actes externes malveillants** sont à l'origine de presque un quart des violations notifiées. Ce type d'incidents a 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 et notamment les membres de la direction dans les structures de taille moyenne ou petite : 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. Ces actes sont souvent la conséquence d'une méconnaissance du cadre légal ou technique et donnent fréquemment lieu à des plaintes auprès du parquet.

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, …).

Nature de l'impact

La quasi-totalité des violations de données ont un impact en rapport avec la perte de confidentialité des données concernées. Nous notons l'apparition de cas mixtes concernant les attaques de type « ransomeware » qui combinent une perte de disponibilité mais aussi de plus en plus régulièrement une perte de confidentialité suite à l'exfiltration partielle ou totale des données. Les responsables de traitement sont généralement en difficulté face à l'analyse de ce type d'incident, principalement à cause du niveau de détail des logs disponibles insuffisant ou inadapté.

Analyse structurelle

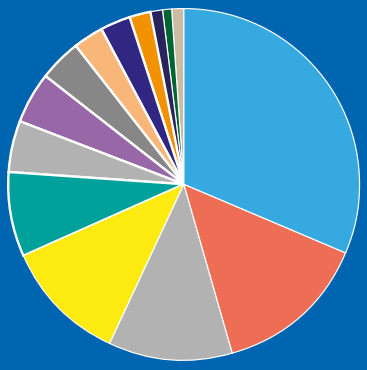
Le secteur de la santé, de par la sensibilité et le volume d'informations qu'il traite rencontre un nombre significatif d'incidents de sécurité impliquant des données personnelles. Le COVID-19 et les traitements informatiques y relatives ont encore accentué cet état. Toutefois, nous notons les efforts de ce secteur et plus particulièrement des délégués à la protection des données, afin de traiter et prévenir ces incidents par la sensibilisation du personnel ou encore les travaux d'harmonisation sur les méthodologies d'analyse du risque.

Dans le domaine des banques et assurances, les responsables de traitement semblent avoir des grilles d'analyses du risque très différentes d'un responsable à l'autre amenant ainsi certains d'entre eux, pourtant de taille significative, à ne pas ou peu notifier.

LES ACTIVITÉS EN 2020

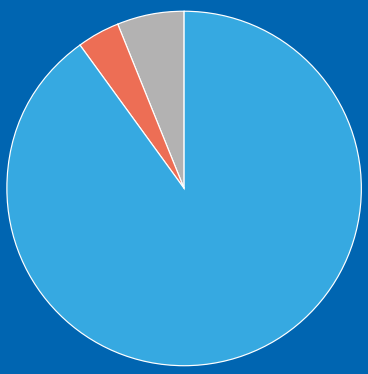
3

NATURE DES INCIDENTS



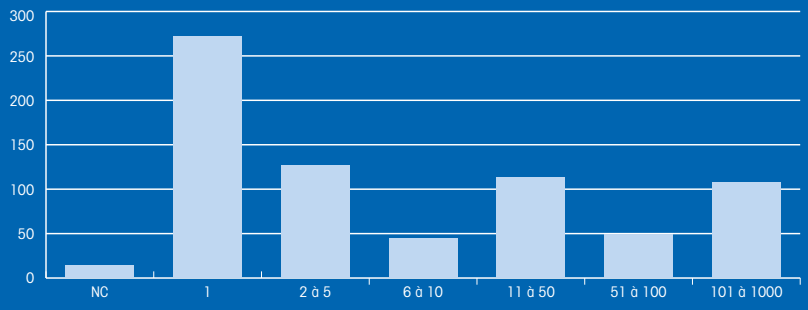
- Données à caractère personnel envoyé au mauvais destinataire (33 %)
- Piratage, hacking (15 %)
- Divulgation de la donnée personnelle de la mauvaise personne (12 %)
- Publication involontaire (12 %)
- Dispositif perdu ou volé (8 %)
- Phishing, hameçonnage (5 %)
- Problème technique (4 %)
- Papiers perdus, volés, endroit non sécure (3 %)
- Mail perdu, ouvert (3 %)
- Malware, logiciel malicieux (2 %)
- Communication verbale non autorisée (1 %)
- Destruction incorrecte de données personnelles sur papier (1 %)
- Autres (1 %)

NATURE DE L'IMPACT



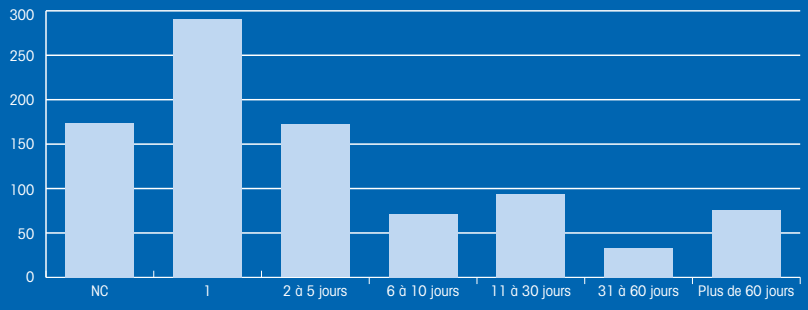
- Confidentialité (90 %)
- Disponibilité (4 %)
- Intégrité (6 %)

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)

Les petites et moyennes entreprises ont parfois des difficultés à appréhender le processus de gestion des notifications tant dans la prévention des incidents que dans leur gestion. Le secteur de la vente de biens immobiliers est une parfaite illustration de cette problématique.

Plus de la moitié des incidents de sécurité sont détectés au plus tard 5 jours après leur survenance. Toutefois, la CNPD a constaté que presque 10 % 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.

LES ACTIVITÉS EN 2020

3

VIOLATIONS DE DONNÉES DANS LE SECTEUR DES COMMUNICATIONS ÉLECTRONIQUES

Conformément au règlement (UE) n°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 2020, aucune violation de données dans le secteur des communications électroniques n'a été signalée à la CNPD.

RÉTENTION DE DONNÉES DE TRAFIC ET DE LOCALISATION

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

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

- les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,
- le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,
- les cas dans lesquels les demandes de données n'ont pas pu être satisfaites.

En 2020, les autorités compétentes ont fait 2 990 demandes auprès des opérateurs. Ce chiffre a légèrement augmenté (+13 %) par rapport à l'année 2019 où 2 601 demandes avaient été faites.

LES ACTIVITÉS EN 2020

3

8 CONTRÔLER ET ADOPTER DES MESURES CORRECTRICES

Pour veiller au respect de la législation applicable en matière de protection des données, la Commission nationale dispose de pouvoirs d'enquête pour vérifier l'application des règles en matière de protection des données. En cas de traitement contraire à la règlementation, la CNPD peut adopter des mesures correctrices (p.ex. avertissement, rappel à l'ordre, limitation temporaire, définitive, ou interdiction du traitement, imposition d'une amende administrative etc.).

La CNPD peut lancer des enquêtes suite à des réclamations (démarche réactive) ou de sa propre initiative (démarche proactive). Ces enquêtes peuvent être menées sous la forme de contrôles sur place ou sous forme d'audits. Quand la CNPD souhaite vérifier la conformité par rapport à une thématique spécifique du RGPD, les enquêtes peuvent prendre la forme de campagnes de contrôle sur place ou d'audits auprès d'un échantillon d'organisations sélectionnées sur base de critères de risque, comme par exemple le secteur d'activité ou la taille de l'organisation, le nombre de personnes concernées ou le type de données traitées.

Le pouvoir d'enquête permet à la CNPD d'obtenir du responsable du traitement ou du sous-traitant l'accès à :

- toutes les données à caractère personnel qui sont traitées et, de manière générale, toutes les informations nécessaires à l'exercice de sa mission ;
- tous les locaux, notamment toute installation et tout moyen de traitement.

Le règlement relatif à la procédure d'enquête adoptée par la CNPD le 22 janvier 2020, en même temps que son règlement d'ordre intérieur, précise le déroulement d'une telle enquête (voir encadré).

Tout en prenant en compte le principe du contradictoire, ce règlement définit les différentes étapes du déroulement d'une enquête de la décision d'ouverture par le Collège des commissaires siégeant en formation plénière, en passant par son instruction jusqu'à la communication des griefs éventuellement soulevés par le chef d'enquête.

La décision à l'issue d'une enquête est finalement prise par le Collège des commissaires siégeant en formation restreinte (la « Formation Restreinte ») sur base des propositions du chef d'enquête formulées dans la communication des griefs.

Au premier semestre de l'année 2020, la CNPD a transposé les dispositions du règlement relatif à la procédure d'enquête à l'ensemble des enquêtes en cours depuis 2018 et un nombre important de propositions de décisions a été transféré à la Formation Restreinte pour prise de décision.

Il est à noter qu'en comparaison avec les années précédentes, le nombre d'enquêtes (contrôles et audits) a été peu élevé en raison des restrictions relatives à la pandémie.

CONTRÔLES

La CNPD réalise des contrôles sur place proactifs dans le cadre de campagnes thématiques (vidéosurveillance et COVID-19 – voir ci-après) ou des contrôles réactifs suite à des incidents notifiés, des réclamations reçues, des informations relayées dans les médias ou faisant suite à un contrôle précédent.

Ces contrôles se font moyennant des visites sur place non annoncées au préalable.

La CNPD a effectué 8 visites sur place en 2020. Ces enquêtes portaient sur le domaine de la vidéosurveillance et la régularité des traitements en lien avec la lutte contre le COVID-19.

Fin 2020, les dossiers d'enquête de la campagne de contrôle concernant la **vidéosurveillance et la géolocalisation** débutée en 2018 ont été transmis à la Formation Restreinte qui a adopté ses premières décisions début 2021.

Par ailleurs, la CNPD a lancé, début décembre 2020, une campagne de contrôle afin de vérifier la conformité par rapport au RGPD de la **collecte et de l'utilisation de données à caractère personnel mises en place par les organisations dans le cadre des mesures qu'elles ont prises pour lutter contre la propagation de la pandémie COVID-19**. Cette campagne s'inscrit dans la continuité du suivi par la CNPD des particularités et risques spécifiques en termes de protection des données induits par la pandémie COVID-19. Les visites sur site de cette campagne ont débuté en décembre 2020 pour se prolonger au cours de l'année 2021 sur un échantillon de 20 organisations publiques et privées de toutes tailles et issues de secteurs d'activité divers.

AUDITS

Avec l'entrée en application du RGPD, la CNPD a également mis en place des enquêtes selon la méthodologie d'audit, particulièrement bien adaptée quand il s'agit de vérifier le respect de la législation sur la protection des données à caractère personnel dans un cadre organisationnel ou technique plus complexe.

Comme pour les contrôles sur place, les audits peuvent être organisés soit de façon réactive dans le contexte d'une enquête décidée suite à une réclamation reçue, soit de façon proactive sous la forme de campagne thématique portant sur des obligations choisies du règlement. De telles campagnes d'audits réalisées auprès d'organismes sélectionnées sur base de critères d'échantillonnage spécifiques à la thématique choisie, permettent à la CNPD d'évaluer le niveau de conformité des organismes à la protection des données.

Vu l'impact du nouveau rôle du délégué à la protection des données et l'importance de son intégration dans l'entreprise, la CNPD avait décidé de lancer un premier audit thématique en septembre 2018 sur la fonction de **délégué à la protection des données** (DPD). L'objectif de cette campagne était de vérifier la conformité des organismes aux obligations du RGPD en matière de désignation du DPD, de ses missions et de ses fonctions.

En 2020, 21 dossiers (sur 25 au total) ont été transférés à la Formation Restreinte qui prendra ses décisions à l'issue de chacune de ces enquêtes. Une grande partie de ces décisions seront prises au cours de l'année 2021. En plus des décisions individuelles publiées de façon anonymisée, il est prévu de publier les résultats de cette campagne sous forme de lignes directrices ou de recommandations afin de permettre aux responsables de traitements ou sous-traitants de bénéficier des bonnes et d'éviter les mauvaises pratiques identifiées au cours des audits.

Un audit sur le thème de la **transparence** a été lancé en 2020 et 6 enquêtes auprès d'entreprises du secteur du commerce électronique ont été ouvertes dans ce cadre.

La transparence n'est pas une nouvelle notion mais un principe et une obligation bien ancrés en matière de protection des données personnelles. Son objectif premier est l'installation de la confiance entre les responsables du traitement et les personnes concernées. La notion de transparence prend toutefois une dimension encore plus forte avec le RGPD et le nouveau principe de redevabilité (« accountability »), auquel elle est intrinsèquement liée. Le principe de transparence permet aux personnes concernées de contrôler leurs données à caractère personnel et d'exiger des responsables de traitement qu'ils rendent des comptes à cet égard.

Le secteur du e-commerce a été ciblé dans le choix des entreprises à auditer. En effet, de par les spécificités même du secteur, la transparence revêt un caractère plus important. Une autre motivation qui a guidé la CNPD à choisir ce thème a été le fait que le secteur du e-commerce a connu une croissance exceptionnellement forte lors de la pandémie et en période de confinement.

MESURES CORRECTRICES

Dans le cadre de ses missions, la CNPD dispose, entre autres, du pouvoir d'adopter les mesures correctrices prévues à l'article 58.2 du RGPD (p.ex. avertissement, rappel à l'ordre, mise en conformité, limitation temporaire, définitive, ou interdiction du traitement, etc.), y inclus le pouvoir d'imposer des amendes administratives en application de l'article 83 du RGPD en complément ou à la place des autres mesures correctrices en fonction des caractéristiques propres à chaque cas.

Les violations par le responsable du traitement du RGPD peuvent faire l'objet d'amendes administratives 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 néanmoins que les sanctions soient « effectives, proportionnées et dissuasives » - ceci impliquant que dans chaque cas d'espèce, les éléments énumérés à l'article 83.2 du RGPD soient pris en compte, comme par exemple la nature, la gravité et la durée de la violation, le nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi, les catégories de données à caractère personnel concernées par la violation ou encore le fait que la violation a été commise délibérément ou par négligence.

Une mesure correctrice ne peut être prononcée que par la Commission nationale siégeant en formation restreinte lorsqu'elle prend une décision sur l'issue d'une enquête conformément à l'article 41 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.

Les premières décisions de la Commission nationale siégeant en formation restreinte sur l'issue d'enquêtes menées depuis 2018 seront prises et publiées en 2021.

LES ACTIVITÉS EN 2020

3

LA PROCÉDURE D'ENQUÊTE DE LA CNPD

L'ouverture d'une enquête peut être proposée à tout moment par un membre du Collège conformément à l'article 38 de la loi du 1er août 2018 précitée. Il soumet cette proposition au Collège qui l'approuve endéans un délai d'un mois à la majorité des voix et qui désigne un membre du Collège, à l'exception du président, en tant que chef d'enquête.

Le dossier d'enquête est alors instruit par le chef d'enquête sur base des informations, déclarations et/ou pièces collectées lors de l'enquête y compris au moyen des éventuels entretiens et/ou demandes d'informations complémentaires. A l'issue de l'instruction, le chef d'enquête retient les violations alléguées au RGPD qu'il entend matérialiser sous forme de griefs. Les griefs sont alors transmis au contrôlé qui aura la possibilité d'y répondre de manière contradictoire.

Ces éventuels échanges sont inclus au dossier d'enquête qui sera transmis à la Formation Restreinte. Dans le cas de figure où le chef d'enquête n'identifie ou ne retient aucun grief, il transmet à la Formation Restreinte une proposition de clôture.

En vertu de l'article 10 2° b) du Règlement d'ordre intérieur de la CNPD adopté par décision n°3AD/2020 du 22 janvier 2020, la Commission nationale siégeant en formation restreinte informe le contrôlé de la date de la séance au cours de laquelle est inscrite l'affaire le concernant et de la faculté qui lui est offerte d'y être entendu. Lors de ladite séance, le chef d'enquête est entendu pour présenter des observations orales sur l'affaire et, lorsqu'il assiste à la séance, le contrôlé est invité à présenter des observations orales.

Suite à ces séances, la Commission nationale siégeant en formation restreinte prend l'affaire en délibéré. Les décisions qu'elle prend sont publiées de façon anonyme, sauf si une anonymisation n'est pas possible ou si la CNPD a décidé d'appliquer l'article 52 de la loi précitée du 1er août 2018, c'est-à-dire d'ordonner la publication d'une décision de manière intégrale et nominative.

9 CONTRÔLER LES TRAITEMENTS DE DONNÉES DES AUTORITÉS RÉPRESSIVES OU DE SÉCURITÉ NATIONALE

En application 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, la CNPD est aussi compétente pour contrôler les traitements de données opérés par les autorités répressives ou les autorités de sécurité nationale, telles que la Police grand-ducale, le Service de renseignement de l'État, l'Autorité nationale de sécurité ou l'Administration des Douanes.

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 prévoit par ailleurs que le rapport annuel de la CNPD doit comprendre 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.

DEMANDES D'INFORMATION

La CNPD a traité 22 demandes d'information écrites ou orales en matière de traitement de données dans le domaine répressif et de sécurité nationale. La moitié des demandes concernaient l'exercice des droits des personnes concernées, en particulier le droit d'accès. Sans prétendre à l'exhaustivité, la CNPD a également été sollicitée pour répondre à des questions en matière pénale ou de sécurité publique en matière de vidéosurveillance dans les lieux publics et dans les lieux privés, de l'utilisation des dashcams sur la voie publique et le traitement de données à caractère personnel en vue du dépôt d'une plainte pénale.

LES ACTIVITÉS EN 2020

3

Dans le contexte du « Fichier central », la CNPD a participé à plusieurs réunions du groupe de suivi des *« recommandations formulées par la CNPD et l'IGP relatives aux traitements de données à caractère personnel effectués par la Police grand-ducale »*, composé de représentants de la Police grand-ducale, de l'Inspection générale de la police, du Ministère de la sécurité intérieure, du Ministère de la Justice, du Parquet général et de la CNPD.

La CNPD a participé à une réunion avec le Service national de la prévention de la criminalité de la Police grand-ducale au sujet de la vidéosurveillance dans les habitations privées.

AVIS

La CNPD a adopté 4 avis relatifs aux traitements de données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Il s'agit de prises de position concernant :

- la vidéosurveillance à des fins policières (VISUPOL) (2 avis) ;
- la création de l'Autorité nationale de sécurité ;
- le système de contrôle et de sanction automatisés (radars aux feux rouges).

L'avis concernant « VISUPOL » est résumé ci-après. Les autres avis peuvent être consultés sur le site de la CNPD à l'adresse https://cnpd.public.lu/fr/publications/rapports/index.html.

Vidéosurveillance à des fins policières (VISUPOL)

La CNPD a avisé le projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

Le projet de loi a pour objet de conférer au dispositif de vidéosurveillance policière un cadre légal suite à l'abrogation de la base légale encadrant ce dernier avec l'entrée en application 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.

Dans les remarques générales quant au champ d'application du projet de loi, la CNPD a salué le choix du gouvernement d'encadrer légalement l'installation, la gestion et l'exploitation de caméras dans l'espace public par la Police grand-ducale prenant ainsi l'exemple de ses voisins, la Belgique, l'Allemagne et la France. Néanmoins, la Commission nationale a constaté que le gouvernement avait adopté une approche restrictive relative à l'installation

de dispositifs de vidéosurveillance ayant une finalité de sécurité publique, en limitant son utilisation à la Police. Les responsables des communes, également nombreux à vouloir se doter de tels dispositifs afin de veiller à la sécurité des espaces publics de leurs communes ne peuvent donc installer de telles mesures de surveillance. La CNPD a rappelé que le système de vidéosurveillance policière dénommé « VISUPOL » était limité au territoire de la Ville de Luxembourg. Par conséquent, pour qu'une commune, en tant que responsable du traitement, puisse installer un dispositif similaire dans les espaces publics et ce à des fins de sécurité publique, il faudrait un texte légal lui offrant une telle possibilité. A cet égard, la Commission nationale a recommandé de prendre exemple sur les législateurs belges et français.

Dans ses commentaires de l'article 1er du projet de loi ajoutant un nouvel article 43 bis à la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, la CNPD a notamment souligné l'impératif de respecter le droit ainsi que la jurisprudence de l'Union européenne.

En effet, la Commission nationale a salué les efforts déployés quant au respect des principes d'accessibilité et de transparence du projet de loi ainsi que la qualité de ce dernier, en particulier en ce qui concerne la délimitation des lieux publics présentant des risques et l'autorisation ministérielle quant à l'installation du dispositif VISUPOL dans ces derniers.

Enfin, en termes de proportionnalité du traitement de données et de garanties appropriées pour la sauvegarde des droits et libertés fondamentaux des citoyens, la CNPD a considéré que les procédés de masquage du système VISUPOL doivent inclure l'intérieur d'un lieu privé. En ce qui concerne la durée de conservation des images collectées, la Commission nationale a considéré que le délai de deux mois était proportionné au regard des finalités poursuivies.

RÉCLAMATIONS

La CNPD a été saisie de 11 réclamations en matière pénale et de sécurité nationale dans des cas où les responsables du traitement n'ont pas fait droit, n'ont pas répondu du tout ou ont répondu de manière insuffisante à des demandes d'accès aux données de personnes concernées. Ce chiffre reste comparable à celui de l'année 2019 où la CNPD avait reçu 10 réclamations dans ce domaine.

NOTIFICATION DE VIOLATIONS DE DONNÉES

Les responsables du 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 ACTIVITÉS EN 2020

3

Entre le 20 août 2018 (entrée en vigueur 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) et le 31 décembre 2020, la CNPD a reçu deux notifications de violations de données concernant des traitements de données à caractère personnel en matière pénale, ainsi qu'en matière de sécurité nationale.

CONTRÔLES PRÉVUS PAR DES DISPOSITIONS LÉGALES SPÉCIFIQUES

En matière pénale et de sécurité nationale, certaines dispositions législatives nationales et européennes prévoient que la CNPD effectue des visites sur place et/ou audits spécifiques et réguliers.

Dans ce contexte, et sur base de l'article 43 de la loi du 18 juillet 2018 sur la Police grand-ducale, la CNPD a entamé en 2019 un audit des accès à certains fichiers étatiques des membres de la Police ayant la qualité d'officier de police judiciaire ou d'officier de police administrative. Cet audit, toujours en cours en raison de la pandémie COVID-19, couvre notamment les aspects suivants : attribution des accès, respect du principe « need to know, need to do », disponibilité de journaux et motifs des consultations.

La CNPD doit par ailleurs procéder tous les quatre ans à des audits de protection des données au niveau des parties nationales des systèmes d'information européens (Schengen Information System) SIS II et VIS (Visa Information System (VIS) ainsi qu'à des revues régulières des logs de ces systèmes d'informations.

COOPÉRATION EUROPÉENNE

La supervision coordonnée du traitement des données dans les systèmes d'information de l'UE et par les organes, offices et agences européens sera progressivement transférée des groupes de coordination (tels que le Groupe de coordination du contrôle du SIS II ou le Groupe de coordination du contrôle du système d'information européen des Douanes) au Comité de Supervision Coordonnée (CSC), créé en décembre 2019 et opérant depuis sous l'égide de l'EDPB.

Le CSC réunit dans ses réunions biannuelles les autorités de contrôle de l'UE, le Contrôleur européen de la protection des données (EDPS), ainsi que les autorités de contrôle des États membres Schengen non membres de l'UE lorsque le droit de l'UE le prévoit.

L'objectif principal du CSC est d'assurer la surveillance coordonnée des systèmes d'information de l'UE et des organes, bureaux et agences de l'UE dans les domaines des frontières, de l'asile et des migrations (SIS, EES, ETIAS et VIS), de la coopération policière et judiciaire (SIS, Parquet européen, Eurojust, ECRIS-TCN) et du marché intérieur (IMI).

Les tâches du Comité consistent, notamment, dans le soutien à fournir aux autorités de contrôle dans la réalisation d'audits et d'inspections, l'élaboration de travaux sur l'interprétation ou l'application des actes juridiques de l'UE concernés et de propositions de solutions harmonisées, l'étude de problèmes liés à l'exercice d'un contrôle indépendant ou à l'exercice et la promotion des droits des personnes concernées.

En 2020, le Comité a publié son programme de travail pour la période de 2020 à 2022 avec comme activités planifiées :

- la promotion des droits des personnes concernées ;
- l'examen des difficultés d'interprétation ou d'application du droit communautaire et national ;
- l'échange des informations ;
- la réalisation d'audits conjoints ou d'inspections coordonnées ;
- la préparation de la supervision au démarrage des activités du Parquet européen et des autres organes de l'UE et systèmes d'information qui relèveront du champ d'application du CSC au futur.

LES ACTIVITÉS EN 2020

3

10 CONTRIBUER AUX TRAVAUX INTERNATIONAUX DANS LE DOMAINE DE LA PROTECTION DES DONNÉES

L'activité de la Commission nationale a été marquée par une forte participation aux travaux européens, dominés par des dossiers complexes et techniques.

La Commission nationale, représentée par un ou plusieurs de ses agents, a participé en 2020 à de nombreux groupes de travail au niveau européen et international. Il s'agissait notamment :

- du Comité européen de la protection des données (EDPB ou European Data Protection Board) qui regroupe toutes les autorités européennes ainsi que le Contrôleur européen à la protection des données (EDPS ou European Data Protection Supervisor) ;
- de la conférence internationale des commissaires à la protection des données et de la vie privée.

Les réunions de travail et conférences suivantes auxquelles la CNPD participe régulièrement ont dû être annulées en raison de la pandémie :

- le « Groupe de Berlin », dédié à la protection des données dans le secteur des communications électroniques ;
- la conférence des commissaires européens à la protection des données ;
- le séminaire européen « Case Handling Workshop ».

EUROPEAN DATA PROTECTION BOARD (EDPB)

L'EDPB 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, en anglais « European Data Protection Supervisor » (EDPS).

L'EDPB est institué par le règlement général sur la protection des données 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 l'EDPS. Un Protocole d'accord définit les conditions de la coopération entre l'EDPB et l'EDPS.

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.

LES ACTIVITÉS EN 2020

3

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.

L'EDPB a adapté sa façon de travailler dans le contexte de la pandémie et organisé 27 réunions plénières dont 25 à distance rassemblant ses membres (en ce compris la CNPD), par rapport à 11 réunions plénières par année en moyenne depuis sa création. Ce nombre de réunions s'explique notamment par l'intensification du travail d'une part, en raison des questions émergentes dans le contexte de l'épidémie de COVID-19 en matière de protection des données, et, d'autre part, de par les tâches juridiques et l'arrêt Schrems II rendu le 16 juillet 2020 par la Cour de Justice de l'Union européenne qui a mis en cause le mécanisme/pratiques de transferts de données à caractère personnel vers des États tiers de nombreux acteurs.

Participation de la CNPD aux sous-groupes (« Expert SubGroups »)

A côté des réunions plénières, les autorités de protection des données de l'Union européenne se réunissent au sein de sous-groupes thématiques (juridiques et informatiques).

La CNPD a donc assuré sa participation aux travaux et continue d'être représentée au sein de tous les sous-groupes d'experts thématiques et réseaux du Comité qui sont au nombre de 14, ainsi qu'aux réunions biannuelles du Comité de Supervision Coordonnée (CSC).

Il s'agit des sous-groupes (« Expert SubGroups ») suivants :

- Border, Travel and Law Enforcement (BTLE) ;
- Compliance, e-Government and Health (CEH) ;
- Cooperation (COOP) ;
- Enforcement (ENF) ;
- Financial Matters (FMESG) ;
- Fining Taskforce (FINES) ;
- International Transfer (ITS) ;
- IT User ;
- Key Provisions (KEYP) ;
- Strategic Advisory (SAESG) ;
- Social Media (SOCM) ;
- Technology (TECH).

La CNPD a également contribué au travail de deux taskforces. L'une est chargée d'examiner les plaintes déposées à la suite de l'arrêt Schrems II de la CJUE et l'autre, de l'élaboration des recommandations pour aider les

responsables du traitement et les sous-traitants dans leur tâche consistant à déterminer et à mettre en œuvre des mesures supplémentaires appropriées pour garantir une protection adéquate lors du transfert de données vers des pays tiers.

L'autorité de contrôle luxembourgeoise a ainsi participé en 2020 à 115 réunions de groupes de travail dont 100 à distance sans compter les réunions en équipe de rédaction. Avec les réunions plénières, cela revient à un nombre global de 142 réunions. La CNPD a quotidiennement assuré le suivi des dossiers traités au niveau du Comité au niveau des groupes et s'est impliquée dans la rédaction de divers projets de lignes directrices en assumant le rôle de rapporteur.

A côté de nombreux autres projets en cours, **la CNPD a assumé le rôle du rapporteur** pour les projets suivants finalisés en 2020 :

- Document sur la procédure d'approbation des critères de certification par l'EDPB aboutissant à une certification commune, le sceau européen de protection des données ;
- Guidance sur l'analyse des critères de certification ;
- Avis sur les critères d'accréditation de la CNPD pour les organismes de certification ;
- Avis sur les critères d'accréditation de l'autorité de contrôle du Royaume-Uni pour les organismes de certification ;
- Evénement pour les parties prenantes dans le cadre du projet de lignes directrices sur l'intérêt légitime ;
- Lignes directrices sur l'interaction du texte de la directive PSD2 et du RGPD ;
- Document sur les termes de référence du groupe d'experts de soutien de l'EDPB.

La CNPD a continué ses contributions aux travaux en cours en 2020 sur les documents suivants :

- Lignes directrices sur la « blockchain » ;
- Utilisation et conservation des données de cartes de crédit ;
- Lignes directrices sur les assistants vocaux ;
- Lignes directrices sur les droits des personnes concernées.

En cours de l'année, la CNPD a organisé et modéré 5 ateliers de travail sur la certification sous RGPD dans le cadre de la mise en place de ces activités à l'EDPB. L'objectif de ces ateliers était de préparer les membres de l'EDPB à la possibilité d'émettre des avis sur les critères de certification sous l'article 64.1.c du RGPD. Le résultat de ces travaux à conduit à la rédaction de la guidance EDPB sur l'évaluation des critères de certification, dont la CNPD était également le rapporteur.

La CNPD s'est également portée volontaire pour contribuer aux travaux en cours sur les lignes directrices sur l'intérêt légitime.

LES ACTIVITÉS EN 2020

3

Documents adoptés en 2020

L'EDPB a adopté de nombreux documents de travail, guidances et lettres. Certains de ces documents sont résumés ci-dessous. Ils peuvent tous être téléchargés dans leur version complète sur Internet[6].

Contribution à l'évaluation du RGPD par la Commission européenne

Dans le cadre de l'évaluation du RGPD par la Commission européenne, toutes les autorités membres du Comité, y inclus la CNPD, ont contribué par des réponses individuelles à un questionnaire sur l'évaluation du RGPD deux années après sa mise en application adressé par la Commission Européenne au Comité. Sur base de ces réponses individuelles, les membres de l'EDPB ont élaboré une réponse commune à la Commission européenne.

Le Comité conclut dans la communication qu'il est prématuré de réviser le RGPD. Il est convaincu que la coopération entre les autorités de contrôle aboutira à une culture commune et à une pratique cohérente et en présente des solutions possibles mais reconnait en même temps les difficultés dans l'application du RGPD issues de la mosaïque de procédures nationales. En juin 2020, la Commission européenne confirme les analyses du Comité.

Lignes directrices

L'EDPB a adopté 9 nouvelles lignes directrices visant à clarifier l'éventail de dispositions du RGPD. Les lignes directrices adoptées concernaient :

- les véhicules connectés et les applications liées à la mobilité ;

  Les lignes directrices se concentrent sur le traitement des données à caractère personnel en relation avec l'utilisation non professionnelle de véhicules connectés par les personnes concernées.

- les transferts de données à caractère personnel entre autorités et organismes publics de l'EEE et non membres de l'EEE ;

  Cette guidance vise à fournir des orientations concernant l'application de l'article 46, paragraphe 2, point a), et paragraphe 3, point b), du RGPD ayant trait aux transferts de données à caractère personnel d'autorités ou organismes publics de l'EEE à des organismes publics de pays tiers ou à des organisations internationales, dans la mesure où ceux-ci ne sont pas couverts par une décision d'adéquation prise par la Commission européenne. Les organismes publics peuvent choisir d'utiliser ces mécanismes, que le RGPD considère comme étant mieux adaptés à leur situation, mais ils sont aussi libres de s'en remettre à d'autres outils pertinents offrant des garanties appropriées conformément à l'article 46 du RGPD.

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

- le consentement ;

  Ces lignes directrices fournissent une analyse approfondie de la notion de consentement dans le RGPD. La notion de consentement telle qu'utilisée jusqu'à présent dans la Directive sur la protection des données (« directive 95/46/CE ») et dans la Directive « vie privée et communications électroniques » a évolué. Le RGPD apporte des clarifications et des précisions complémentaires sur les conditions d'obtention et de démonstration d'un consentement valable.

- l'interaction entre la deuxième directive sur les services de paiement (DSP2) et le RGPD ;

  Le Comité clarifie les rôles, les conditions dans lesquelles les nouveaux prestataires de services d'initiation de paiement (PSIP) et prestataires de services d'information sur les comptes (PSIC) pour lesquelles la DSP2 introduit le cadre juridique, peuvent accéder aux informations sur les comptes de paiement. Les lignes directrices pour lesquelles la CNPD était rapporteur en 2020, rappellent que le traitement de données sensibles est en principe interdit, si le responsable du traitement n'a pas obtenu le consentement explicite de la personne concernée ou si le traitement est nécessaire pour des motifs d'intérêt public important.

- les concepts de responsable du traitement et de sous-traitant ;

  Ces lignes directrices donnent des orientations sur la question de savoir selon quels critères qualifier les différents acteurs en tant que responsable de traitement, sous-traitant ou responsable du traitement conjoint. Le document apporte des clarifications importantes sur l'évolution de ces concepts en raison de l'entrée en vigueur du RGPD et de plusieurs arrêts de la Cour de Justice de l'Union européenne. Les lignes directrices sont complétées par des illustrations graphiques permettant plus aisément la compréhension des différents concepts.

- le ciblage des utilisateurs des médias sociaux ;

  Ces lignes directrices visent à fournir des orientations pratiques aux parties prenantes et contiennent divers exemples de situations permettant à ces parties prenantes d'identifier rapidement le « scénario » le plus proche de la pratique de ciblage qu'elles entendent déployer. Le document vise à clarifier notamment les rôles et les responsabilités du fournisseur de médias sociaux et à recenser les risques potentiels pour les droits et libertés des personnes concernées.

- les objections pertinentes et motivées ;

  Dans le cadre du mécanisme de coopération établi par le RGPD, les autorités de contrôle ont le devoir d'échanger toute information utile et de coopérer en s'efforçant de parvenir à un consensus. Conformément à l'article 60,

paragraphes 3 et 4, du RGPD, l'autorité de contrôle chef de file est tenue de soumettre un projet de décision (« draft decision ») aux autorités de contrôle concernées, lesquelles peuvent alors soulever une objection pertinente et motivée dans un délai spécifique.
Deux options s'offrent à l'autorité de contrôle chef de file lorsqu'elle reçoit une objection pertinente et motivée (« reasoned and relevant objection»). Si elle ne suit pas cette objection ou estime qu'elle n'est pas motivée ou pertinente, elle saisit le Comité de la question dans le cadre du mécanisme de contrôle de la cohérence (article 65 du RGPD). Lorsqu'au contraire, l'autorité de contrôle chef de file entend suivre l'objection et soumet un projet de décision révisé, les autorités de contrôle concernées peuvent exprimer une objection pertinente et motivée sur le projet de décision révisé dans un délai de deux semaines.

Cette ligne directrice a permis de définir plus précisément ce qui est entendu par « objection pertinente et motivée ».

Travaux ciblant les traitements de données à caractère personnel dans le cadre de la lutte contre l'épidémie de COVID-19

Dans le contexte de la pandémie, l'EDPB a entrepris de conseiller les gouvernements, autorités, responsables du traitement et développeurs de solutions numériques afin de leur permettre de surmonter les défis posés par la crise sanitaire du COVID-19 tout en respectant les droits fondamentaux à la protection des données et à la vie privée.

Ci-après une sélection des travaux finalisés par le Comité rendus public au cours de l'année :

- Dans les lignes directrices relatives à l'utilisation de données de localisation et d'outils de recherche de contacts pour lutter contre le COVID-19, le Comité répond à certaines initiatives prises par les gouvernements afin de combattre la pandémie, notamment l'utilisation des données de localisation ou de la recherche des contacts, en indiquant lesquelles peuvent en être des finalités acceptables tout en insistant sur les principes d'efficacité, de nécessité et de proportionnalité ;
- La déclaration sur l'impact de la protection des données sur l'interopérabilité des applications de traçage de contacts contient une analyse plus approfondie des aspects essentiels, notamment la transparence, la base juridique, le statut de responsable du traitement, les droits des personnes concernées, la conservation et la minimisation des données, la sécurité de l'information et l'exactitude des données dans le cadre de la création d'un réseau interopérable d'applications ;
- Les lignes directrices sur le traitement des données de santé à des fins de recherche visent à éclairer des questions juridiques urgentes qui émergeaient dans le contexte de l'épidémie de COVID-19 concernant l'utilisation des données de santé ;
- L'EDPB a donné une suite à une demande de consultation de la Commission européenne concernant son projet de lignes directrices sur les applications de soutien à la lutte contre la pandémie de COVID-19. Dans sa réponse, l'EDPB a abordé spécifiquement l'utilisation des applications pour la fonction de recherche des contacts et

d'alerte. Dans ce domaine, une attention accrue doit être accordée à la minimisation de l'impact sur la protection de la vie privée tout en permettant le traitement des données dans le but de préserver la santé publique ;
- La déclaration sur les droits des personnes concernées en rapport avec l'état d'urgence dans les États membres rappelle essentiellement les grands principes applicables aux limitations des droits des personnes concernées et rappelle que, même en cas d'état d'urgence, la protection des données à caractère personnel doit être préservée dans toutes les mesures d'urgence d'un État de droit. Suivant la déclaration, le Comité avait également donné un mandat au sous-comité « Key Provisions » de travailler sur des lignes directrices sur les limitations des droits des personnes concernées en générale. Ces lignes directrices ont été soumises à consultation publique ;
- La déclaration sur le traitement des données à caractère personnel dans le cadre de la réouverture des frontières Schengen à la suite de la pandémie de COVID-19 vise particulièrement des mesures tels que le dépistage du COVID-19, l'exigence de certificats délivrés par des professionnels de la santé et l'utilisation d'une application de traçage volontaire des contacts.

Coopération européenne dans le cadre du Brexit

La préparation du Brexit dont l'impact sur les frontières, la libre circulation et l'échange des données entre les forces de l'ordre des États membres et du Royaume-Uni a fait l'objet de plusieurs déclarations et notes d'informations qui ont été publiées sur le site du Comité.

L'EDPS a publié une déclaration sur la fin de la période de transition du Brexit, dans laquelle il décrit les principales implications de la fin de cette période pour les responsables du traitement des données et les sous-traitants. Le Contrôleur européen de la protection des données a notamment insisté sur la question des mécanismes de transferts de données vers un pays tiers ainsi que sur les conséquences dans le domaine de la surveillance réglementaire et du mécanisme de guichet unique.

Recommandations

L'EDPB a émis des recommandations sur les garanties essentielles européennes pour les mesures de surveillance et sur les mesures qui complètent les outils de transfert pour garantir le respect du niveau de protection des données à caractère personnel de l'UE.

Ces recommandations, auxquelles la CNPD a fourni son support au sein de la taskforce dédiée, ont comme objectif **d'aider les exportateurs de données de se conformer à l'arrêt Schrems II** ce qui nécessite d'identifier et mettre en œuvre des mesures supplémentaires efficaces là où elles sont requises. Il s'agit donc de permettre des transferts licites de données à caractère personnel vers des pays tiers tout en garantissant que les données transférées bénéficient d'un niveau de protection essentiellement équivalent à celui garanti dans l'EEE.

Les recommandations contiennent une feuille de route des étapes que les exportateurs de données doivent suivre et une liste non exhaustive d'exemples de mesures supplémentaires et des conditions dans lesquelles elles peuvent être efficaces.

Ce document doit être lu à la lumière des recommandations sur les garanties essentielles européennes fournissant aux exportateurs de données des éléments leur permettant de déterminer si le cadre juridique régissant l'accès des autorités publiques aux données à des fins de surveillance dans les pays tiers peut être considéré comme une ingérence justifiable dans les droits à la vie privée et à la protection des données à caractère personnel.

Les deux documents ont été soumis à consultation publique après leur adoption. Une version finale va être adoptée en 2021.

Avis relatif à la cohérence

Afin de garantir l'application cohérente du RGPD dans les affaires ayant des implications transfrontières, l'EDPB a émis **31 avis relatifs à la cohérence**.

Ces avis concernaient notamment les projets de listes soumis par des autorités de contrôle concernant des opérations de traitement pour lesquelles une AIPD est requise, ainsi que celles pour lesquelles aucune AIPD n'est requise. Les autres avis portaient sur les clauses contractuelles types, les règles d'entreprise contraignantes (BCR), les compétences des autorités de contrôle et les critères d'agrément des organismes chargés du suivi des codes de conduite ou de la certification.

Les premiers avis sur les critères d'accréditation des organismes de certification ont été adoptés par le Comité. La CNPD a soumis ses critères d'accréditation (« GDPR CARPA ») à l'EDPB en même temps que l'autorité du Royaume-Uni. Elle a été co-rapporteur avec le secrétariat EDPB pour l'avis rendu sur les critères d'accréditation de l'autorité du Royaume-Uni, tandis que cette dernière a été co-rapporteur avec le secrétariat EDPB pour l'avis rendu sur les critères d'accréditation de la CNPD. Ces avis visent à établir une approche cohérente et harmonisée concernant les exigences que les autorités de contrôle et les organismes d'accréditation nationaux appliqueront lors de l'accréditation des organismes de certification. Ces travaux constituent une étape importante vers la délivrance par l'EDPB des avis d'approbation des critères de certification et donc vers le sceau européen de protection des données.

Les lignes directrices sur l'analyse des critères de certification pour lesquelles la CNPD était rapporteur en 2020 vont soutenir les efforts des autorités de contrôle dans la promotion et la mise en œuvre du sceau européen de protection des données.

Décisions contraignantes

L'EDPB agit également comme un organe de règlement des litiges et émet des décisions contraignantes. En 2020, il a émis sa première décision contraignante concernant un différend qui est apparu suite au projet de décision de l'autorité irlandaise concernant la société Twitter.

Nouveau registre des décisions prises par les autorités nationales

L'EDPB a publié sur son site web un nouveau registre contenant les décisions prises par les autorités nationales de protection des données à la suite de la procédure de coopération avec le mécanisme de « guichet unique » (Article. 60 du RGPD).

Sous le RGPD, les autorités de contrôle ont le devoir de coopérer dans les affaires ayant une composante transfrontalière afin de garantir une application cohérente du RGPD. Dans le cadre de ce **mécanisme du « guichet unique »** (en anglais « OSS » ou « One-Stop-Shop mecanism »), l'autorité de contrôle chef de file est en charge de préparer les projets de décision et travaille avec les autres autorités de contrôle concernées pour parvenir à un consensus.

Jusqu'à début juin, les autorités de contrôle ont adopté 110 décisions dans le cadre du mécanisme de guichet unique. Le registre comprend l'accès aux décisions ainsi que des résumés des décisions en anglais préparés par le secrétariat de l'EDPB. Ce registre sera une source d'information importante pour les praticiens de la protection des données qui auront accès à des informations montrant comment les autorités de contrôle collaborent pour faire appliquer le RGPD dans la pratique. Les informations contenues dans le registre ont été validées par les autorités chef de file en question et conformément aux conditions prévues par les législations nationales.

Stratégie 2021-2023

A la fin de l'année 2020, l'EDPB a adopté sa stratégie 2021-2023, qui définit les objectifs stratégiques du Comité, rassemblés autour de quatre piliers, ainsi que trois actions clés par pilier pour aider à réaliser ces objectifs.

Les quatre piliers de la stratégie du EDPB sont les suivants :

- promouvoir l'harmonisation et faciliter le respect des règles ;
- soutenir l'application effective des règles et la coopération efficace entre les autorités nationales de surveillance ;
- une approche des nouvelles technologies fondée sur les droits fondamentaux ;
- la dimension mondiale.

La stratégie sera également mise en œuvre au moyen d'un programme de travail, qui détaillera davantage les actions de l'EDPB. Ce programme de travail sera adopté au début de l'année 2021.

Dans le cadre de sa stratégie 2021-2023, l'EDPB a décidé de créer un groupe d'experts de soutien sur la base d'un projet pilote « Support Pool of Experts » (SPE). L'objectif est d'apporter un soutien matériel à ses membres sous forme d'expertise utile pour les enquêtes et les activités de contrôle de l'application des règles et d'améliorer la coopération et la solidarité entre les membres de l'EDPB en partageant, renforçant et complétant les points forts, ainsi qu'en répondant aux besoins opérationnels.

GLOBAL PRIVACY ASSEMBLY

La « Global Privacy Assembly » (GPA) » est un forum d'échanges à l'échelle mondiale, où 130 membres partagent des bonnes pratiques et adoptent des positions communes. Crée en 1979, elle était connue sous le nom de « International Conference of Data Protection and Privacy Commissioners » (ICDPPC) jusqu'en 2019. Ce changement de nom reflète la volonté de cette assemblée de renforcer sa visibilité et sa position en tant qu'acteur effectif et influent au niveau international.

La CNPD a participé à l'édition 2020 « At your desk » de la conférence internationale de la Global Privacy Assembly. Initialement prévue au Mexique, la 41ème conférence s'est déroulée en ligne en 3 séances de 3 heures du 13 au 15 octobre 2020.

Les autorités de protection des données ainsi que quelques ONG ont réfléchi ensemble sur les défis posés par le COVID-19 en matière de protection de données et vie privée.

Les discussions ont porté sur des enjeux importants comme par exemple :

- l'interopérabilité mondiale des lois et réglementations relatives à la protection des données et à la protection de la vie privée ;
- l'élaboration d'approches novatrices de coopération en matière de réglementation pour relever les défis de l'IA ;
- le rapport entre la protection des données et d'autres droits et libertés ;
- les moyens pour améliorer la coopération entre les autorités en matière d'enquêtes ;
- la promotion de la coopération entre les autorités chargées de la protection des données, de la protection des consommateurs et de la concurrence ;
- les moyens pour aborder la protection de la vie privée et des données dans l'éducation numérique et la protection de la vie privée des enfants.

La CNPD a contribué aux groupes de travail suivants :

L'édition 2020 « At your desk » de la conférence internationale de la « Global Privacy Assembly ». De gauche à droite : Jérôme Commodi, Tine A. Larsen, Marc Lemmer et Romy Schaus.

- Digital Education Working Group : support technique pour la réorganisation et revitalisation de la plateforme de partage d'outils pédagogiques CIRCABC ;
- Policy Strategy Working Group : co-rédaction du Digital Economy Background Paper ;
- Cadre légal et pratiques des autorités de protection des données relatifs à l'exercice des droits des mineurs ;
- COVID-19 related Privacy and Data Protection Issues Working Group : Résolution sur les défis liés à la vie privée et à la protection des données dans le contexte de la pandémie COVID-19.

Plusieurs résolutions ont été adoptées lors de la conférence internationale. La CNPD était co-sponsor de deux d'entre elles :

- la résolution sur l'aide humanitaire internationale et
- la résolution relative aux déclarations communes sur les questions mondiales émergentes.

Une des résolutions les plus marquantes était celle sur les défis liés à la **vie privée et à la protection des données dans le contexte de la pandémie de COVID-19.**

Dans cette résolution, les membres du GPA ont reconnu l'important travail accompli par la taskforce COVID-19 pour identifier via un sondage parmi les membres de l'assemblée, les problèmes liés à la protection de la vie privée qui sont apparus à la suite de la pandémie :

- le « contact tracing », y compris le traçage numérique des contacts, qui était la préoccupation la plus pressante des juridictions ;
- le traitement des données des salariés dans des situations de travail à domicile et de retour au travail ;
- le traitement des données des enfants/étudiants associées à l'utilisation des technologies de formation et de scolarisation en ligne ;
- l'échange de données sur la santé entre les hôpitaux, les ministères de la santé et d'autres organismes gouvernementaux compétents.

La taskforce a élaboré un compendium de bonnes pratiques dans le contexte de la pandémie. Il est conçu comme un document susceptible d'être actualisé par les membres du GPA.

Selon la résolution, les autorités de protection des données devraient continuer à jouer un rôle central en fournissant des conseils et une assistance aux gouvernements, aux organisations compétentes et aux autres parties prenantes sur la façon de traiter et de partager les données à caractère personnel dans le contexte de la pandémie.

Une des décisions de la résolution est de prendre appui sur les travaux réalisés par la taskforce et de créer un nouveau groupe de travail temporaire (Groupe de travail sur les questions de protection des données et de la vie privée liées au COVID-19), doté d'un mandat initial d'un an. Ce groupe de travail aura notamment comme mission de formuler des recommandations et coordonner les réponses du GPA sur les questions qui se posent dans le contexte de la pandémie COVID-19 et sur la voie du rétablissement.

Le « Digital Education Working Group »

La priorité de ce groupe de travail est de sensibiliser davantage les enfants, les adolescents et les adultes aux questions de protection des données, car cela renforce leur capacité à revendiquer leurs droits à la protection des données dans le monde numérique.

Un outil de bibliothèque électronique permet de partager entre autorités de protection des données (APD) au niveau mondial du matériel pédagogique sur la protection de la vie privée disponible et d'autres ressources en ligne provenant aussi bien des autorités que d'autres parties prenantes. La plateforme CIRCABC de la Commission européenne héberge cet outil en ligne créé en 2015.

La CNPD, ensemble avec son homologue français, la CNIL, a défini et mis en œuvre le projet de revitalisation de la libraire en ligne afin d'assurer qu'elle reste efficace et attrayante. Le but du projet est l'amplification de l'utilisation faite par les autorités, la promotion de l'outil, la diffusion des éléments didactiques y stockés et l'encouragement des autorités à s'inspirer de ce matériel pour l'utilisation dans leur pays.

En tant que co-administrateurs, les deux autorités ont mis à jour la plateforme et mis en place une nouvelle classification par type de formation et de ressources et avec des nouvelles catégories.

CONFÉRENCE DE PRINTEMPS DES AUTORITÉS EUROPÉENNES À LA PROTECTION DES DONNÉES ET LE SÉMINAIRE « EUROPEAN CASE HANDLING WORKSHOP »

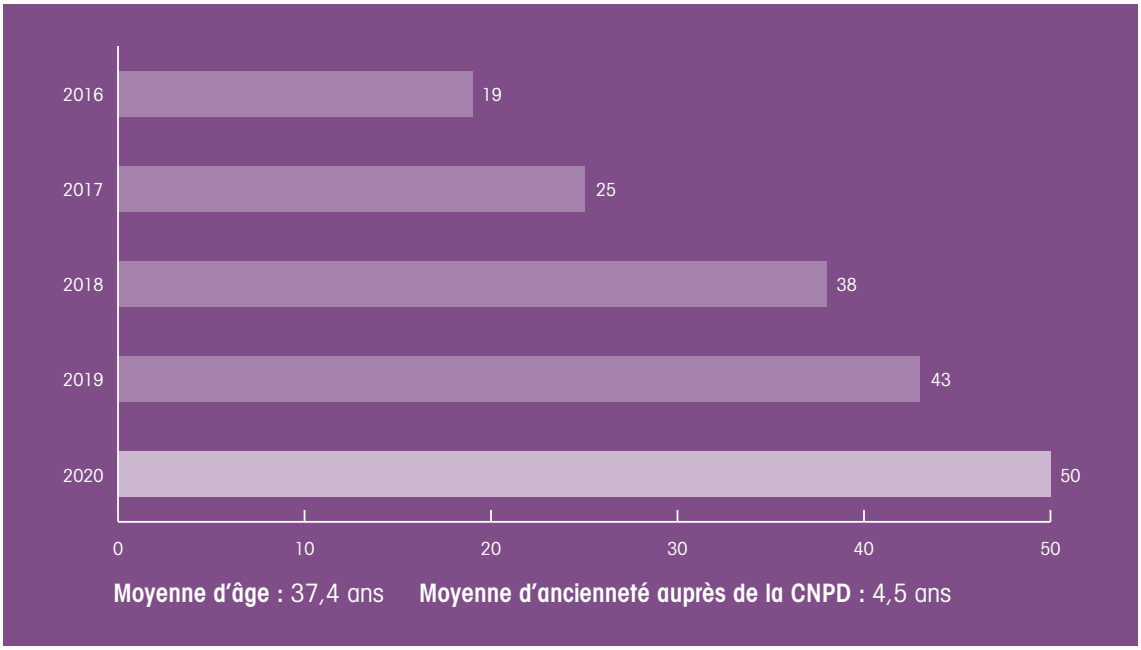
En raison de l'épidémie du COVID-19, la Conférence des autorités européennes de protection des données 2020 ainsi que le séminaire « European Case Handling Workshop » ont dû être reportés. Un groupe de travail a été rétabli qui a pour objectif de définir une vision d'avenir pour la Conférence. Le groupe est composé de représentants de la Croatie, du Royaume-Uni, CEPD, de l'Allemagne, de la Suisse, des Pays-Bas et les deux hôtes précédents, à savoir l'Albanie et la Géorgie.

Pour éclairer les travaux du groupe, les membres de la Conférence, dont fait partie la CNPD, ont contribué en indiquant dans un questionnaire des propositions concernant leurs idées quant à l'objectif et l'orientation futurs de la Conférence.

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

1 RESSOURCES HUMAINES



Collège
Tine A. LARSEN, Présidente

Thierry LALLEMANG, Commissaire

Christophe BUSCHMANN, Commissaire

Marc LEMMER, Commissaire

Dani JEITZ,
Juriste - Secrétaire du Collège
« Formation plénière »

Claudia FETZ,
Juriste - Secrétaire adjointe du Collège
« Formation Restreinte »

Membres suppléants
Michèle BRAM,
Directrice adjointe de l'Institut Luxembourgeois de Régulation (ILR)

Martine KRAUS,
Vice-Présidente auprès du Tribunal d'arrondissement de Luxembourg

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

Data Protection Officer
Bertrand NAVARRE,
Juriste, Délégué à la protection des données

Relation internationales
Romy SCHAUS,
Juriste, Chargée des relations européennes et internationales

Service Administration
Tine A. LARSEN,
Présidente

Thierry RIES,
Chef de service

Jan KUFFER,
Chef d'Unité « IT interne & Logistique »

Maryse WINANDY,
Chef d'unité « Réception/Secrétariat »

Cristina FERREIRA DA CUNHA,
Rédacteur-stagiaire, Comptabilité et finances

Anna MAGI,
Rédacteur, Ressources humaines

Stéphanie MATHIEU,
Rédacteur, Secrétariat

Service Sensibilisation
Marc LEMMER,
Commissaire

Tom KAYSER,
Chef d'unité « Communication externe »

Roberta RIBEIRO OERTEL,
Chef d'unité « Sensibilisation & Formation »

Alexandre KUHN, Expert IT,
Veille juridique et technologique

Vincent LEGELEUX, Expert IT,
Veille juridique et technologique

Service Guidance
Thierry LALLEMANG,
Commissaire

Arnaud HABRAN,
Chef de service et Chef d'unité « Transferts pays tiers »

Francis MAQUIL,
Chef d'unité « Demandes d'informations »

Carmen SCHANCK,
Chef d'unité « Avis juridiques »

Mathilde STENERSEN,
Chef d'unité « Ligne directrices thématiques »

Nina BURMEISTER,
Juriste, Demandes d'informations

Céline DEROOSE,
Juriste, Demandes d'informations

Marie DOUZAL,
Juriste, Avis juridiques

Kalliroi GRAMMENOU,
Juriste, Transferts pays tiers

Christian WELTER,
Juriste, Demandes d'informations

Service Conformité
Marc LEMMER,
Commissaire

Alain HERRMANN,
Chef de service et Chef d'unité « Avis Analyses d'Impact », « Certifications » et « Codes de Conduite »

Service Réclamations
Thierry LALLEMANG,
Commissaire

Laurent MAGNUS,
Chef de service et Chef d'unité « Réclamations nationales »

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

Georges WEILAND,
Chef d'unité « Réclamations européennes »

Sabrine ABAAB,
Juriste, Réclamations européennes

Jessica BLEEK,
Juriste, Réclamations européennes

Gaël DUMORTIER,
Juriste, Réclamations nationales

Barbara GIROUD,
Juriste, Réclamations nationales

Nicolas RASE,
Juriste, Réclamations nationales

Service Enquêtes
Christophe BUSCHMANN,
Commissaire

Michel SINNER,
Chef de service et Chef d'unité « Contrôles »

Edith MALHIERE,
Chef d'unité « Audits »

Sébastien TEISSEIRE,
Chef d'unité « Notifications de violations de données »

Christine ANDRES,
Enquêteur, Audits

Solène BENNET,
Enquêteur, Audits

Jérôme COMMODI,
Enquêteur, Contrôles

Fanny DRATSCHMIDT,
Enquêteur, Audits

Marie-Laure FABBRI,
Enquêteur, Audits

Florent KLING,
Enquêteur, Contrôles

Marc MOSTERT,
Enquêteur, Contrôles

Bao-Khanh NGUYEN TRUNG,
Enquêteur, Contrôles

François RICHALET,
Enquêteur, Audits

Mathieu RINCK,
Enquêteur, Audits

Céline SIMON-HERTZ,
Enquêteur, Contrôles

Maximilian WELSCH,
Enquêteur, Contrôles

Assermentations en 2020 de Mathilde Stenersen, Francis Maquil et Romy Schaus. De gauche à droite : Thierry Lallemang, Mathilde Stenersen, Francis Maquil, Tine A. Larsen, Christophe Buschmann, Romy Schaus et Marc Lemmer.

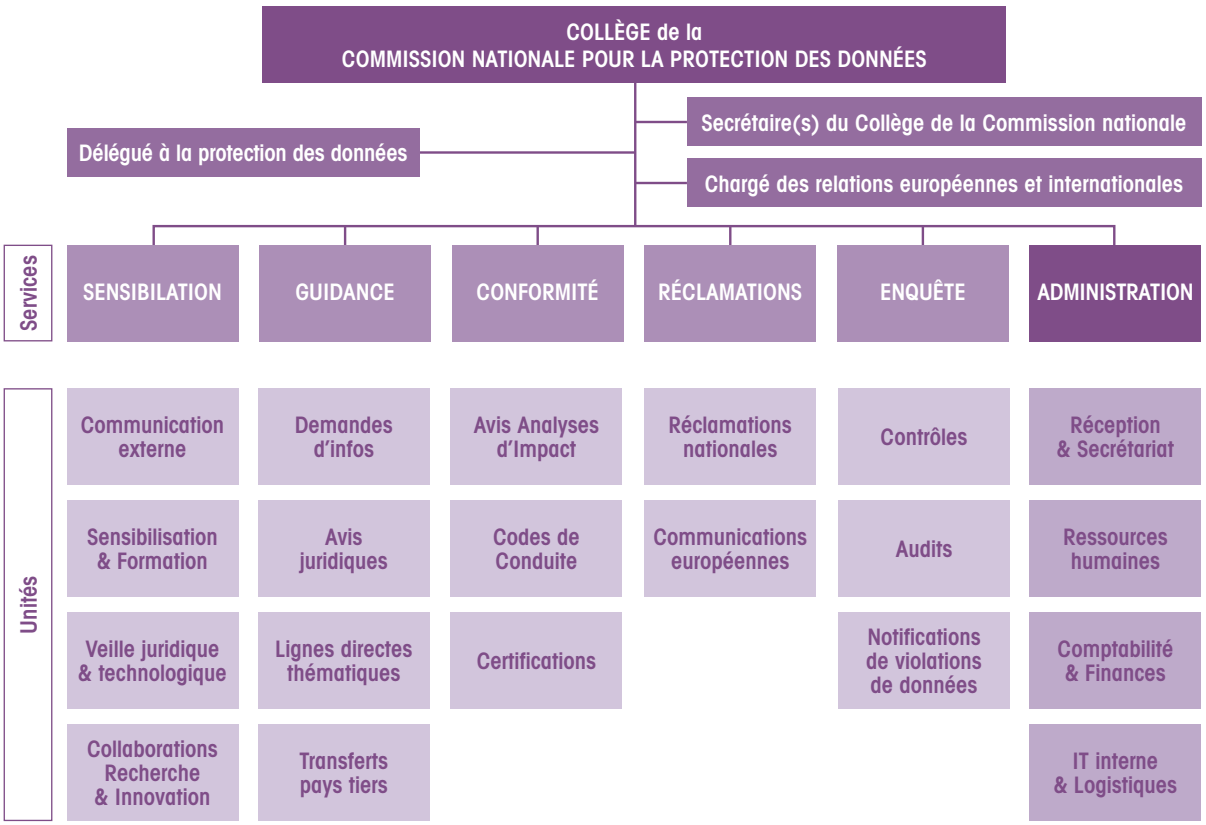
RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

2 ORGANISATION DE LA CNPD

Fin 2019, la CNPD a réorganisé ses services et a adapté son organigramme afin de mieux pouvoir assurer ses missions et de faciliter la lisibilité de ses activités et de son organisation.

L'organigramme ci-dessous est en vigueur depuis le 1er janvier 2020.



Adoption du règlement d'ordre intérieur, de la procédure relative aux réclamations et de la procédure relative aux enquêtes

En 2020, la CNPD a adopté plusieurs documents importants concernant son organisation interne et ses procédures de travail. Il s'agit notamment du règlement d'ordre intérieur (ROI), de la procédure relative aux réclamations (décrite plus en détail dans la partie II.6. du présent rapport) et de la procédure relative aux enquêtes (décrite plus en détail dans la partie II.8. du présent rapport).

Le règlement d'ordre intérieur de la CNPD a été adopté en application des articles 32 paragraphe (1er) et 33 de la loi organique du 1er août 2018 et définit les conditions de fonctionnement, l'organisation des services et les règles de procédure applicable devant la CNPD.

Le **chapitre 1er** décrit les conditions de fonctionnement de la CNPD et notamment la composition, les affaires courantes, la représentation vers l'extérieur, la gestion financière et le déroulement des séances de délibération du Collège.

L'organisation des services et la structure générale de la Commission nationale sont présentées dans le **chapitre 2**. Il s'agit plus particulièrement des services « Sensibilisation », « Guidance », « Conformité », « Réclamations », « Enquêtes » et « Administration ». Par ailleurs, ont été définies les fonctions suivantes directement attachées à la Commission nationale : le(s) secrétaire(s) du Collège, le chargé aux relations européennes et internationales et le délégué à la protection des données.

Le **chapitre 3** définit les procédures applicables devant la CNPD dans les cas suivants :

- Notification d'une violation de données à caractère personnel ;
- Consultation préalable ;
- Notification de la désignation du délégué la protection des données ;
- Approbation des codes de conduites ;
- Agrément des organismes de suivi des codes de conduite ;
- Approbation de critères de certification ;
- Agrément des organismes de certification ;
- Autorisations des clauses contractuelles et des arrangements administratifs ;
- Approbation des règles d'entreprise contraignantes ;
- Introduction d'une réclamation ;
- Demandes d'avis préalable dans le cadre de l'article L. 261-1 du Code du travail ;
- Enquêtes ;
- Voies de recours.

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

3 RAPPORT DE GESTION RELATIF AUX COMPTES DE L'EXERCICE 2020

En mai 2020, après avoir mené une réflexion stratégique et prévisionnelle sur son fonctionnement et ses missions, la Commission nationale pour la protection des données (CNPD) a adopté le document *« Stratégie et programme de travail 2020-2022 »*. Ledit document lui permettra de mieux planifier, coordonner et suivre ses activités pendant la période afférente et d'améliorer ainsi la gestion de ses ressources.

C'est précisément dans cet ordre d'idées, qu'un nouvel organigramme avait d'ores et déjà été adopté par le Collège de la CNPD en janvier 2020, lui permettant de faire face non seulement aux défis d'un monde numérique, mais également au changement de paradigme engendré par le règlement général sur la protection des données (RGPD) et qui s'exprime par le basculement du contrôle a priori vers un contrôle a posteriori.

La structure ainsi arrêtée prévoit depuis lors et mis à part le secrétariat du Collège, le chargé des relations européennes et internationales ainsi que le délégué à la protection des données, les six services suivants :

- Sensibilisation ;
- Guidance ;
- Conformité ;
- Réclamations ;
- Enquêtes et
- Administration.

Après le renforcement des effectifs opéré entre 2015 et 2018 en guise de préparation aux changements engendrés par la nouvelle règlementation européenne sur la protection des données, le document stratégique vise dorénavant à consolider les équipes opérationnelles. Il s'agit à présent d'étoffer les ressources des différents services en fonction de leurs besoins respectifs, besoins estimés à un effectif total de 62 ETP (équivalent temps plein) par rapport à un effectif total autorisé de 54 ETP en décembre 2020. A noter que dans le souci d'optimiser le fonctionnement de la CNPD, l'effectif total aurait dû atteindre 62 ETP en 2023. Or, au vu de la réduction de la dotation attribuée à la CNPD pour l'exercice 2021 et suivants, les recrutements prévus pour les années 2021 à 2023 ont dû être reportés aux exercices 2025 à 2027.

Concernant les dépenses de l'exercice 2020, il est à noter que les chiffres en question ne sauraient être considérés comme représentatifs en raison de deux facteurs ayant largement influencés le fonctionnement et par conséquent les dépenses de la CNPD.

Il s'agit d'abord et bien évidemment de la crise sanitaire et des mesures qui en découlent, mais aussi de l'aménagement et du déménagement vers le nouveau siège de la CNPD.

Si la crise sanitaire a eu pour conséquence une diminution de certaines catégories de dépenses, l'aménagement des nouveaux locaux et le déménagement ont généré des frais supplémentaires.

Le budget

Le budget de la CNPD s'est élevé pour l'exercice 2020 à un montant de 7.667.224 €, soit une progression de 40,88 % par rapport au budget de de l'année précédente. L'augmentation de 2.224.808 € par rapport à 2019 résulte principalement du renforcement des effectifs qui représentent en effet 84,73 % du budget total. S'y ajoutent en outre le loyer et les charges locatives du nouveau siège, alors que les anciens locaux étaient mis à disposition par le Fonds Belval au prix des charges.

Les dépenses

Au cours de l'exercice 2020, le total des dépenses de l'établissement public s'est élevé à 6.336.137 € par rapport à 4.799.182 € en 2019, soit une augmentation de 32,03 %, tout en restant en dessous du crédit budgétaire accordé et se chiffrant à 7.667.224 €.

L'excédent budgétaire s'explique essentiellement par une moins-value pour charges relatives au personnel en raison du fait que suite à la crise sanitaire et en vue du déménagement vers le nouveau siège, tous les recrutements prévus dès janvier 2020 ont dû être reportés en fin d'année, voire en début de l'année suivante.

A noter que les dépenses relatives à l'aménagement du nouveau siège s'élevant à 509.946 € ne sont comprises ni dans le total des dépenses, ni dans le montant du crédit budgétaire accordé pour l'exercice 2020 repris ci-dessus. En effet, et conformément à la décision du Collège prise lors de la séance plénière du 27 mai 2020, le financement afférent a été réalisé moyennant affectation de la plus-value de l'exercice 2019.

1. Actif immobilisé

Dans le respect de l'article 46 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 disposant que « les comptes de la CNPD sont tenus selon les règles de la comptabilité commerciale », les dépenses en rapport avec l'acquisition de mobilier, de logiciels et de matériel informatique ont été comptabilisées au bilan de l'établissement public ; leur amortissement étant enregistré parmi les frais de fonctionnement.

En 2020, le mobilier supplémentaire nécessaire dans le cadre de l'aménagement des nouveaux bureaux a engendré une dépense de 70.644 €.

Les dépenses en vue de l'acquisition de nouveaux équipements informatiques se sont élevées à 21.681 €, alors qu'en 2019 aucune dépense correspondante n'a été enregistrée.

2. Frais de fonctionnement

Les frais de fonctionnement se sont élevés à 806.279 € par rapport à 405.529 € en 2019, soit une augmentation de 400.750 € respectivement 98,82 %, sans pour autant dépasser les prévisions budgétaires initiales d'un montant de 1.033.260 €.

2.1. Frais généraux

La progression précitée de 98,82 % résulte notamment du fait que, suite à l'augmentation de ses effectifs et vu l'impossibilité du Fonds Belval d'offrir une solution à court terme aux besoins de la CNPD, cette dernière s'est vue contrainte de se diriger vers une location sur le marché privé. Si l'ancien siège avait été gracieusement mis à disposition par le Fonds Belval, la CNPD doit désormais supporter le coût du loyer relatif à ses nouveaux locaux situés dans l'immeuble NAOS, ainsi que les charges locatives afférentes. En 2020, les frais en question se sont élevés à 547.657 €, soit une augmentation de 392.870 € par rapport à 2019 où les dépenses à charge de ce poste au montant de 154.787 € comprenaient essentiellement le loyer du nouveau siège (en cours d'aménagement) dû pour les mois d'octobre à décembre 2019.

Les dépenses se rapportant aux équipements et fournitures de bureau se chiffrent à 19.924 €. La progression de 13,74 % par rapport à 2019 suit le renforcement des effectifs opéré fin 2019 et au cours de l'année 2020.

Avec l'emménagement dans les nouveaux locaux, les frais d'aménagement et d'entretien afférents sont passés de 21.097 € en 2019 à 42.335 € pour l'année 2020. Vu que la surface du nouveau siège dépasse substantiellement celle de l'ancien, les frais en rapport avec le nettoyage quotidien ont augmenté en conséquence.

Les frais de documentation ont diminué de 37,28 % pour tomber de 10.716 € en 2019 à 6.721 € pour l'exercice 2020. Il en est de même pour ce qui est des frais de port et de télécommunication qui se sont chiffrés en 2020 à 10.426 € par rapport à 11.418 € en 2019, soit une diminution de 8,69 %.

Les frais d'honoraires d'un montant de 34.253 € comprennent les dépenses relatives à la tenue des livres comptables, à la gestion des salaires et à la révision des comptes, montant dépassant de 76,99 % celui des frais de l'exercice 2019 se chiffrant à 19.353 €. Cette progression s'explique d'abord par une augmentation des frais résultant de la gestion des salaires et ensuite par le fait qu'en 2020, ce poste comprenait tant les honoraires revenant au réviseur d'entreprises pour l'année en cours que le solde dû pour l'exercice 2019.

Les autres charges générales d'exploitation au montant de 19.107 € sont restées stables sauf qu'une dépense exceptionnelle à raison de 30.448 € s'y ajoute pour frais de déménagement vers les nouveaux locaux.

2.2. Communication et relations publiques

En raison de la crise sanitaire, toutes les réunions et conférences à l'étranger ont été remplacées par des vidéo-conférences de sorte que les frais de voyage, de représentation et de relations publiques au montant de 9.002 € sont restés largement inférieures aux prévisions budgétaires se chiffrant à 52.000 € et aux dépenses engendrées en 2019 et s'élevant à 61.238 €, soit une réduction de 85,30 %.

Les frais de communication et de publication ont diminué de 33.571 € en 2019 à 23.145 € en 2020 et comprennent entre autres les frais de publication du Rapport annuel 2019 s'élevant à 9.312 € ainsi que les annonces relatives aux vacances de postes se chiffrant à 8.566 €.

En raison de la crise sanitaire, aucune campagne de sensibilisation en matière de protection des données n'a pu être organisée, de sorte que les dépenses à charge de ce poste ont été réduites à zéro, alors qu'en 2019 elles s'élevaient à 29.679 €.

2.3. Frais informatiques

Les frais informatiques se sont élevés en 2020 à 63.261 € par rapport à 61.271 € en 2019 et comprennent à l'instar des années précédentes, l'hébergement par une société spécialisée de l'outil « CNPD Compliance Support Tool », développé par la CNPD en coopération avec le LIST (Luxembourg Institute of Science and Technology) et le Service des Médias et des Communications pour un montant de 54.405 €. S'y ajoutent les frais de maintenance des outils informatiques exploités par le service « Administration ».

Il est à noter que les dépenses de ce poste sont restées en dessous des prévisions budgétaires. En effet, depuis la migration en 2017 des systèmes informatiques vers les services du Centre des technologies de l'information de l'État (CTIE), les frais en question sont restés en dessous des prévisions en raison du fait que la plateforme de travail « Sharepoint » utilisée depuis lors par la CNPD, a pu être développée en utilisant exclusivement des composants standards du CTIE. Il s'ensuit que le système ainsi exploité peut être opéré sur une plateforme standard et mutualisée du CTIE permettant de réduire considérablement les coûts afférents.

3. Frais de personnel

Les rémunérations du personnel liquidées en 2020 se sont élevées à 5.387.440 € par rapport à 4.362.465 € en 2019. Cette progression est due aux recalculs importants résultant de l'abolition de la réduction opérée sur les indemnités de stage ainsi qu'au renforcement du personnel réalisé mi et fin 2019 et au courant de 2020.

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

Outre les quatre commissaires, le cadre du personnel permanent comprenait au 31 décembre 2020 :

- 39 agents du groupe de traitement ou d'indemnité A1 dont 16 fonctionnaires,
- 1 employé du groupe d'indemnité A2 ainsi que
- 5 agents du groupe de traitement ou d'indemnité B1 dont 4 fonctionnaires.

S'y ajoute un employé A1 temporaire occupé sur contrat à durée déterminée.

Malgré une augmentation considérable des effectifs relevée en fin d'année, les dépenses effectives sont restées en dessous des prévisions budgétaires. En effet, avec la crise sanitaire, une partie des recrutements prévus n'ont pu être réalisés qu'en fin d'année, respectivement ont dû être reportés en début de l'année suivante.

Mises à part les rémunérations, les frais de personnel comprennent encore un montant de 4.555 € représentant les dépenses se rapportant à la formation du personnel. La progression par rapport à 2019 des dépenses en question suit l'augmentation du nombre de collaborateurs en activité de service.

4. Autres frais

Il s'agit en l'occurrence des frais engendrés par la voiture de service au montant de 4.242 € soit une diminution de 42,21 % par rapport à 2019 et résultant d'une renégociation avec effet rétroactif du contrat de leasing basé sur les distances effectivement parcourues.

L'amortissement du mobilier et du matériel informatique comptabilisé pour un montant de 37.993 € suit celui des investissements effectués et représente une augmentation de 62,61 % par rapport à 23.365 € pour l'exercice 2019.

S'y ajoutent encore les frais bancaires et charges assimilées au montant de à 3.303 €.

5. Aménagement du nouveau siège

Les dépenses relatives à l'aménagement du nouveau siège de la CNPD se sont élevées à 509.946 € et couvrent entre autres

- le cloisonnement intérieur ainsi que les travaux y liés ;
- le câblage électrique et informatique ainsi que les alimentations et raccordements y relatifs ;
- les menuiseries intérieures et
- la climatisation.

Considérant que l'aménagement du siège a été financé moyennant affectation de la plus-value de l'exercice 2019, les dépenses afférentes sont passées par les charges au lieu d'être comptabilisées en tant qu'immobilisation corporelle.

Les recettes

Si la CNPD ne dispose pas de recettes au sens propre du terme, elle peut néanmoins et en vertu de l'article 47 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, imposer des redevances dans le cadre de ses pouvoirs d'autorisation et de consultation. Bien que la CNPD ait adopté en 2020 un règlement fixant le montant et les modalités de paiement afférentes, aucune redevance n'a été perçue en 2020.

Ainsi les recettes se sont limitées au loyer se rapportant à la sous-location des emplacements de parking compris dans le bail relatif au siège situés au sous-sol du bâtiment NAOS et s'élevant à 20.045 €. S'y ajoute encore un montant de 762 € représentant entre autres la participation aux frais mPass des agents de la CNPD.

Le résultat d'exploitation

Compte tenu de la dotation annuelle de 7.667.224 €, dont la Commission nationale pour la protection des données a bénéficié de la part de l'État en application de l'article 47 de la loi du 1er août 2018 précitée, le résultat d'exploitation de l'établissement public s'élève au 31 décembre 2020 à 934.270 €.

ANNEXES

5

5 ANNEXES

AVIS ET DÉCISIONS

- Avis relatif au projet de loi n°7216B 1) portant transposition de : a) l'article 31 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 ; et b) l'article 1er, point 16, de 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/UE ; 2) portant modification de la loi modifiée du 27 juillet 2003 relative au trust et aux contrats fiduciaires ; et 3) portant abrogation de la loi du 10 août 2018 relative aux informations à obtenir et à conserver par les fiduciaires et portant transposition de l'article 31 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.
  (Délibération n°6/2020 du 28 février 2020) 112

- Avis complémentaire relatif au projet de loi n°7216B portant transposition de l'article 31 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, tel que modifié 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/UE.
  (Délibération n°9/2020 du 3 avril 2020) 129

- Avis complémentaire relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la **Police grand-ducale**.
  (Délibération n°10/2020 du 17 avril 2020) 132

ANNEXES

5

ANNEXES

5

ANNEXES

5

Avis relatif au projet de loi n°7511 relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances.

(Délibération n°2/2020 du 27/01/2020)

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 »*.

Par courrier en date du 23 décembre 2019, Monsieur le Ministre des Finances a invité la Commission nationale à se prononcer sur le projet de loi n°7511 relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances (ci-après le « projet de loi n°7511 »).

Il ressort de l'exposé des motifs que le présent projet de loi a pour objet de par son article unique d'introduire dans la loi modifiée du 7 décembre 2015 sur le secteur des assurances une disposition nationale pour légitimer le traitement de données de santé en matière d'assurances en se basant, conformément à l'article 9 paragraphe (2) lettre g) du RGPD, des motifs d'intérêt public important. Les données de santé sont en effet strictement réglementées par ledit article 9 du RGPD et elles ne peuvent être traitées que si l'une des dix conditions y énumérées est remplie.

Dans le commentaire de l'article unique du projet de loi n°7511, les auteurs du projet de loi argumentent à suffisance de droit pourquoi le consentement des personnes désirant souscrire une assurance ne peut pas être une « base habilitante fiable et solide pour le traitement de données concernant la santé ». Pour cette raison, cette intervention du législateur est un requis essentiel pour lever l'insécurité juridique dans laquelle les compagnies d'assurance se trouvent au stade actuel lorsqu'ils traitent des catégories particulières de données au sens de l'article 9 paragraphe (1) du RGPD et plus particulièrement des données de santé.

En effet, déjà dans son deuxième avis complémentaire du 8 juin 2018[1] concernant le projet de loi n°7184 devenu la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime

[1] Délibération n°423/2018 du 8 juin 2018.

général sur la protection des données, la Commission nationale avait estimé que, même s'il est un fait que les compagnies d'assurance doivent pouvoir traiter des données de santé pour certains types de contrats d'assurance, *« 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, …) »*. Par ailleurs, comme un contrat d'assurance est un contrat d'adhésion, la Commission nationale avait estimé que le consentement n'était pas à considérer comme approprié pour légitimer le traitement de données de santé dans ce contexte, mais qu'une condition de légitimité appropriée aurait pu être celle prévue à l'article 6 paragraphe (1) lettre b) du RGPD (*« le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci »*). Or, il s'avère que le législateur européen n'a pas prévue cette finalité à l'endroit de l'article 9 du RGPD.

La Commission nationale avait d'ailleurs suggéré au législateur d'introduire une disposition au projet de loi n°7184 précité permettant aux compagnies d'assurances de traiter des données de santé, à l'exception de données génétiques, 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. Toutefois, cette proposition de texte n'avait pas rencontré l'assentiment du Conseil d'État qui estimait qu'il s'agit d'une « dérogation nationale, ajoutée à la liste du paragraphe 2 [de l'article 9 du RGPD], que les États membres ne sont pas autorisés à introduire. Le dispositif ne saurait pas non plus être considéré comme introduisant des conditions supplémentaires au sens de l'article 9, paragraphe 4. Le nouveau paragraphe 2 de l'article 66 du projet de loi, dans sa version amendée, n'est dès lors pas conforme à l'article 9 du règlement. Le Conseil d'État doit s'y opposer formellement et en demande la suppression ».[2]

L'article unique du projet de loi n°7511 tel que proposé par le législateur se base quant à lui sur l'article 9 paragraphe (2) lettre g) du RGPD qui dispose que *« 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 ».*

Selon la Commission nationale, cette disposition n'ajoute pas de dérogations à celles prévues à l'article 9 paragraphe (2) du RGPD et ne se base pas sur l'article 9 paragraphe (4) du RGPD permettant 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 »*. Le traitement de données de santé par les compagnies d'assurances et de réassurances peut ainsi être fondé sur base de l'article 9 paragraphe 2 lettre g) du RGPD, sous condition que le droit national prévoit spécifiquement *« des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée »,* ce qui n'est actuellement pas le cas. En d'autres termes, l'objet du projet de loi sous avis vise à combler cette lacune en droit national.

[2] Deuxième avis complémentaire du Conseil d'État du 17 juillet 2018 concernant le projet de loi n°7184.

ANNEXES

5

La CNPD salue le texte du projet de loi sous examen, alors que le point 2 de l'article 181bis de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, introduit par l'article unique du projet de loi n°7511 sous revue, énumère de manière suffisante quelles sont ces mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée qui sont à respecter en cas de traitement de données de santé nécessaire à l'exécution de mesures précontractuelles en matière d'assurance ou de réassurance ou à l'exécution d'un contrat d'assurance ou de réassurance, à l'instar d'autres législations européennes comme par exemple celle de l'Irlande, du Royaume-Uni ou des Pays-Bas.

Toutefois, la Commission nationale constate que le commentaire de l'article unique, ainsi que l'exposé des motifs mentionnent à côté de l'article 9 paragraphe (2) lettre g) du RGPD comme base légale du traitement de données de santé par les assurances l'article 9 paragraphe (4) du RGPD. Or, en raison des explications qui précèdent, elle est d'avis que l'unique base légale applicable en espèces est l'article 9 paragraphe (2) lettre g) du RGPD et elle propose ainsi de supprimer toute référence à l'article 9 paragraphe (4) du RGPD.

Finalement, la CNPD tient à souligner que le projet de loi sous examen n'a pas d'incidence sur l'application des règles du RGPD, c'est-à-dire que toutes les dispositions prévues au RGPD restent applicables aux sociétés d'assurance et de réassurance qui traitent des données de santé conformément à l'article unique du projet de loi n°7511. Notamment, les principes relatifs au traitement des données à caractère personnel énumérés à l'article 5 du RGPD et toutes les obligations générales incombant au responsable du traitement et prévues au chapitre IV du RGPD sont à respecter. Par ailleurs, les personnes concernées, c'est-à-dire les clients et prospects desdites sociétés, disposent de tous les droits prévus aux articles 13 à 22 du RGPD dans les conditions y énumérées et en aucun cas, l'article unique du projet de loi n°7511 pourrait être utilisé en tant que base légale pour contourner le respect des droits précités.

Ainsi décidé à Esch-sur-Alzette en date du 27 janvier 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

Avis relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

(Délibération n°04/2020 du 28 février 2020)

Conformément à l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n°2016/680 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 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 »), à laquelle se réfère l'article 8 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 (ci-après désignée « 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 la Chambre des députés, 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 des données personnelles ».

Par courrier du 5 novembre 2019, le Ministre de la Sécurité intérieure a invité la Commission nationale à se prononcer au sujet du projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale (ci-après désigné « le projet de loi »).

Le projet de loi a pour objet de conférer au dispositif de vidéosurveillance policière un cadre légal suite à l'abrogation de la base légale encadrant ce dernier avec l'entrée en application 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. En effet, celle-ci abroge l'article 17 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, tel que modifié en 2007 (ci-après désignée « la loi du 2 août 2002 »). L'article en question fut le fondement légal de la création et de l'exploitation du dispositif de vidéosurveillance à des fins policières appelé VISUPOL. En application de l'article 17, le règlement grand-ducal du 1er août 2007 autorisait la création et l'exploitation de VISUPOL par la Police grand-ducale au sein de zones de sécurité (ci-après désigné « le règlement d'application »). Le règlement d'application déléguait la fixation des zones de sécurité concernées au ministre ayant dans ses attributions la Police grand-ducale à savoir, le Ministre de la Sécurité intérieure. De surcroît, il est pertinent de mentionner que 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 s'applique aux traitements de données à caractère personnel par la Police grand-ducale dans l'exécution de ses missions[3]. Il s'agit notamment des missions de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou

[3] 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, article 1er paragraphe 2. a).

d'exécution de sanction pénale y compris la protection contre les menaces pour la sécurité publique et la prévention de celles-ci[4].

Le projet de loi se réfère à l'avis de la CNPD du 15 mars 2019 relatif à la vidéosurveillance des espaces et des lieux publics à des fins de sécurité publique[5]. La CNPD s'était alors autosaisie du problème de la base légale encadrant les dispositifs de vidéosurveillance. Dans ledit avis, la Commission nationale adoptait alors une approche globale quant à l'utilisation de dispositifs de vidéosurveillance à des fins policières à savoir, la prévention, la recherche et la constatation des infractions[6].

La CNPD souhaite rappeler que les systèmes de vidéosurveillance effectuent une ingérence dans les droits fondamentaux et les libertés reconnus aux individus. Par conséquent, doter d'une base légale de tels systèmes est crucial afin d'établir des garanties pour les personnes qui sont sujettes à la surveillance et au contrôle qui en émanent. Toutefois, le respect des droits fondamentaux n'est pas absolu puisqu'une ingérence dans ces derniers est reconnue à l'article 52 paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne (ci-après désignée « la Charte »). La Convention européenne des droits de l'Homme (ci-après désignée « la CEDH ») rend également possible ladite limitation tout en la rattachant au respect de la vie privée et familiale à son article 8[7].

I. Remarques générales quant au champ d'application du projet de loi

- Une approche restrictive adoptée par le gouvernement

La CNPD constate que le projet de loi vise à modifier le chapitre V de la loi du 18 juillet 2018 sur la Police, chapitre dédié au traitement des données à caractère personnel en y intégrant un article 43 *bis*.

Dans son avis du 15 mars 2019 relatif à la vidéosurveillance des espaces et des lieux publics à des fins de sécurité publique, la CNPD soulignait d'ores et déjà que dans son ensemble, la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ne prévoyait aucune disposition relative au dispositif de vidéosurveillance. La CNPD salue le choix du gouvernement d'encadrer légalement l'installation, la gestion et l'exploitation de caméras dans l'espace public par la Police grand-ducale. Une telle démarche suit les exemples des pays voisins à savoir la France, la Belgique et l'Allemagne.

En revanche, la CNPD regrette que le projet de loi n'ait pas adopté une approche globale relative à l'installation de dispositif de vidéosurveillance ayant une finalité de sécurité publique[8]. En effet, la Police grand-ducale n'est pas la seule à vouloir gérer, exploiter et utiliser la vidéosurveillance à des fins de sécurité publique. Les responsables des communes sont également nombreux à vouloir se doter de tels dispositifs afin de veiller à la sécurité des lieux publics de leurs communes. A ce titre, il est utile de rappeler que dans son avis du 10 mai 2019 relatif au recours

[4] *Ibidem*, paragraphe 1er.
[5] Délibération n°36/2019 du 15 mars 2019.
[6] Conformément à l'article 17 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (abrogée) et l'article 2 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.
[7] Convention européenne des droits de l'Homme, signée à Rome, le 4.XI.1950, article 8.
[8] Projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, commentaires des articles p.6.

à la vidéosurveillance par les communes, sollicité par Madame la ministre de l'Intérieur, la CNPD faisait état des nombreuses demandes d'informations émanant des responsables communaux quant à l'installation de dispositifs de vidéosurveillance dans l'espace public et du souhait de certains élus de relier leurs communes à VISUPOL. De surcroît, le Ministre de la Sécurité intérieure a récemment souligné que l'intérêt des bourgmestres dans l'installation de dispositifs de surveillance dans les communes persiste[9].

La CNPD a d'ores et déjà constaté dans ses avis précités que la loi communale du 13 décembre 1988[10] et la loi du 18 juillet 2018 sur la Police grand-ducale[11] mettent toutes les deux en exergue les interactions entre la Police et les bourgmestres sans pour autant distinguer leurs compétences respectives dans le cadre du pouvoir de police administrative.

De plus, il est nécessaire de rappeler que pour l'instant, le système de vidéosurveillance policière VISUPOL est limité au territoire de la Ville de Luxembourg et que d'après les informations de la CNPD, une extension de ce dernier à d'autres communes n'est pas envisagé. Or, si une commune souhaite, en tant que responsable du traitement, installer un dispositif similaire dans les espaces publics (couvrant des zones d'une superficie plus ou moins grande comme p.ex. places publiques, parcs communaux, aires de jeux ou de loisirs communales…) à des fins de sécurité publique, incluant de façon générale la sécurité des personnes et des biens, il faudrait qu'un texte légal lui donne cette possibilité. Pour ce faire, la Commission nationale est d'avis que l'ajout d'une telle disposition dans le projet de loi sous examen est indispensable. En effet, le projet de loi sous examen prévoit que seule le directeur général de la Police grand-ducale peut prendre l'initiative, avec l'autorisation du ministre, pour étendre le système de vidéosurveillance VISUPOL à d'autres territoires communaux que celui de la Ville de Luxembourg. Comme plus amplement développé dans ses avis du 15 mars 2019 relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurités publique (délibération n°36/2019) et du 10 mai 2019 relatif au recours de la vidéosurveillance par les communes (délibération n°39/2019), l'installation de caméras vidéo par une commune dans des espaces et lieux publics à des fins de sécurité publique ne serait guère conciliable avec la législation actuelle en matière de protection des données.

La CNPD considère dès lors qu'il serait opportun d'adopter une approche globale quant à la vidéosurveillance à des fins de sécurité publique, choix qui apparaît être adopté par les législateurs belge et français.

- Une approche globale adoptée par les législateurs belge et français

L'interrogation quant à la seule modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale réside également dans le fait que les auteurs du projet de loi se sont inspirés du modèle belge[12].

S'il s'avère que le législateur belge a « retenu de régler la vidéosurveillance à des fins policières dans la loi dédiée à la Police »[13], la CNPD observe que ce dernier a néanmoins opté pour une approche globale quant à la gestion,

[9] Lors de l'émission « Face à face » sur RTL le 15 novembre 2019, disponible à la page : https://www.rtl.lu/radio/face-a-face/a/1431367.html, consultée pour la dernière fois le 25/11/2019.
[10] Articles 67 et 68.
[11] Articles 35 et suivants.
[12] Projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, commentaires des articles p.4.
[13] *Ibidem.*

l'exploitation et l'utilisation de la vidéosurveillance au sens large. En effet, la loi du 21 mars 2018[14] modifie à la fois la loi sur la fonction de police en vue de régler l'utilisation de caméras par cette dernière[15] et la loi du 21 mars 2007 réglant l'installation de caméras de surveillance[16]. A toutes fins utiles, le champ d'application matériel de ladite loi en matière de gestion et d'exploitation de dispositif de vidéosurveillance peut être rappelé. Au chapitre 2, l'article 6 paragraphe 1er de la loi du 21 mars 2018 dispose que : « La présente section règle l'installation et l'utilisation de caméras de manière visible par les services de police ». Au paragraphe 2 du même article, il est ajouté que « les dispositions de la présente section sont applicables aux services de police lorsqu'ils ont accès en temps réel aux images de caméras de surveillance installées par d'autres responsables du traitement, en application de la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance ou d'autres lois, si cet accès implique un enregistrement des images au sein des services de police mêmes. ». Au chapitre 3, l'article 64 de la loi du 21 mars 2018 dispose quant à lui que « la présente loi n'est pas applicable aux caméras de surveillance dont les modalités d'installation et d'utilisation sont réglées par ou en vertu d'une législation particulière, aux caméras de surveillance sur le lieu de travail […], aux caméras de surveillance installées et utilisées par les services publics d'inspection et de contrôle, autorisés expressément par la loi, le décret ou l'ordonnance, qui règle leurs compétences, à utiliser des caméras ou à prendre des prises de vues par film ou vidéo, dans le cadre de leurs missions ».

Il ne fait donc aucun doute que le législateur belge ait choisit une approche globale quant à la vidéosurveillance. Le champ d'application de la loi du 21 mars 2018 concerne aussi bien la gestion et l'exploitation de dispositif de vidéosurveillance par la police que par d'autres responsables de traitement tels que les communes.

Le législateur français a également adopté une approche globale puisque l'article L251-2 du Code de la sécurité intérieure dispose que « la transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques compétentes ». Par autorités publiques compétentes, il s'agit notamment du préfet en tant que dépositaire de l'autorité de l'État et considéré comme autorité de police administrative[17]. Il s'agit également des forces de police et de gendarmerie ainsi que des maires[18].

Par conséquent, la Commission nationale est d'avis qu'il serait opportun de prendre exemple sur les démarches adoptées par les législateurs belges et français en ce qui concerne l'encadrement légal des dispositifs de vidéosurveillance mis en place dans les espaces et lieux publics au Luxembourg à des fins de sécurité publique.

II. Commentaires de l'article 1er du projet de loi ajoutant un nouvel article 43bis à la loi modifiée du 18 juillet 2018 sur la Police grand-ducale

La CNPD rappelle la jurisprudence de la Cour européenne des droits de l'Homme selon laquelle la loi « doit définir l'étendue et les modalités d'exercice du pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi

[14] 21 mars 2018. – Loi modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignements et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière.
[15] Ibidem, chapitre 2.
[16] Ibidem, chapitre 3.
[17] « Quelle est la fonction d'un préfet ? », fiche thématique que l'on retrouve à la page : https://www.vie-publique.fr/fiches/20169-role-du-prefet-departement, consultée pour la dernière fois le 16/02/2020.
[18] La vidéosurveillance – vidéoprotection sur la voie publique, fiche thématique que l'on retrouve à la page : https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique, consultée pour la dernière fois le 16/02/2020.

– pour fournir à l'individu une protection adéquate contre l'arbitraire »[19]. La Cour de justice de l'Union européenne quant à elle souligne l'importance « de prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »[20].

Au titre du respect des principes relatifs au traitement des données à caractère personnel tels qu'ils sont prévus par 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, la CNPD rappelle que les données collectées par les dispositifs de surveillance doivent avoir des finalités déterminées, explicites et légitimes et ne doivent pas être traitées d'une manière incompatible avec ces finalités[21].

Elle constate que l'article 43 *bis* ne fait pas expressément état des finalités des dispositifs de vidéosurveillance à des fins policières. En effet, l'installation desdits dispositifs n'est pas explicitement rattachée aux missions de prévention et de détection de crimes et d'infractions pénales. Cela s'explique certainement par le fait que l'article 43 *bis* s'intègre dans la loi du 18 juillet 2018 sur la Police grand-ducale rendant ainsi implicite le lien entre les missions de la Police avec l'installation de caméra de surveillance.

Il peut également être utile de mentionner que les législations des pays voisins relient explicitement l'utilisation de dispositif de vidéosurveillance aux missions des forces de l'ordre[22]. Par conséquent, la CNPD considère qu'il serait opportun que le législateur luxembourgeois en fasse de même.

- Ad paragraphes (1), (2), (3) et (4) du nouvel article 43bis

La CNPD souhaite rappeler que l'installation de ces dispositifs de vidéosurveillance à des fins policières ou de sécurité publique dans des lieux publics doit répondre à des critères objectifs[23]. A titre d'exemples, le règlement d'application du 1er août 2007 précédemment cité prévoyait que la mise en place de zones de sécurité avait pour objet la prévention, la recherche et la constatation d'infractions pénales[24]. Le découpage des zones de Luxembourg-Ville placées sous surveillance était donc inextricablement lié aux missions de la Police grand-ducale. Le risque et le sentiment d'insécurité ne peuvent être considérés à eux seuls comme des critères objectifs. Il y a lieu de les définir, de les délimiter et de les documenter afin de respecter les principes de prévisibilité et de qualité de la loi tels que prévus par le droit de l'Union européenne.

A la lecture de l'article 43 *bis* paragraphe 1er, la CNPD constate que le critère de la mise en place de l'installation de VISUPOL dans les lieux déterminés est celui du « risque particulier de commission de crimes ou de délits ou d'atteintes à la sécurité des personnes ou des biens ». La CNPD salue l'effort de définition des dits lieux et des risques qu'ils présentent effectué dans le projet de loi. En effet, ces lieux sont délimités sur base de critères tels

[19] Cour EDH, Amann c. Suisse [GC], n°277998/95, 16 février 2000, para, 56.
[20] Arrêt du 6 octobre 2015, Schrems, C-362/14, EU :C :2015 :650, point 91. Voir également en ce sens l'arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :201 :2014 :238, point 54.
[21] Article 3 paragraphe 1 b) de la loi 1er août 208 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.
[22] Code de la sécurité intérieure français, article L251-2 ; Loi du 21 mars 2018. Loi modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, article 8.
[23] Avis de la Commission nationale pour la protection des données relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique du 15 mars 2019, p.3.
[24] Règlement grand-ducal du 1er août 2007 autorisant la création et l'exploitation par la Police d'un système de vidéosurveillance des zones de sécurité, Art. 1er.

que la commission de manière répétée des mêmes types de crimes ou de délits dans des lieux donnés[25], la configuration des lieux favorisant la commission de crimes ou de délits[26], les alentours et abords d'infrastructures où sont organisés régulièrement des évènements d'envergure nationale ou internationale[27] ou encore les lieux pouvant accueillir un grand nombre de personnes[28].

La CNPD salue également le fait que la détermination d'une zone surveillée soit conditionnée par une autorisation ministérielle comprenant trois éléments. Tout d'abord, la lecture combinée de l'article 43 *bis* paragraphes 3 et 4 permet de comprendre que le directeur général de la Police grand-ducale, en tant que responsable du traitement de VISUPOL, se doit d'effectuer une analyse d'impact conformément à l'article 26 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. Cette première étape constitue un progrès considérable par rapport au cadre réglementaire précédent qui ne prévoyait pas une telle mesure. Sont ensuite recueillis les avis du bourgmestre et du procureur d'État territorialement compétents sur base de l'analyse d'impact effectuée. Enfin, le directeur général de la Police grand-ducal est tenu de communiquer au ministre « la justification de la nécessité de la vidéosurveillance », « la délimitation des lieux à surveiller », « le nombre, le type, l'emplacement et le champ de vision des caméras », « une évaluation du nombre de personnes concernées par la vidéosurveillance » ainsi que « le caractère permanant ou non de la vidéosurveillance ». Ces trois éléments sont appréciés par le ministre qui décide de délivrer au non l'autorisation ministérielle d'installer le système VISUPOL dans un lieu donné.

Le fait que le projet de loi sous examen détaille les étapes aboutissant à l'autorisation ministérielle et que celle-ci fasse l'objet d'une publication au journal officiel respecte les principes d'accessibilité et de transparence de la loi ainsi que la qualité de cette dernière.

- Ad paragraphe (5) du nouvel article 43bis

L'article 43 *bis* paragraphe 5 dispose que : *« le système de vidéosurveillance prend en images les personnes circulant dans le champ de vision des caméras et enregistre ces images, ainsi que le jour et l'heure auxquelles les images ont été prises sur un outil informatique »*[29]. Au même paragraphe, il est ajouté que la Police grand-ducale peut avoir *« recours à des techniques de focalisation et à des détections automatiques de situations susceptibles à correspondre à la finalité poursuivie »*.

La CNPD considère que la mention des techniques utilisées permet aux individus sujets à ce type de surveillance d'avoir une idée plus précise du savoir qui est extrait quant à leur déplacement ainsi que les techniques utilisées à ces fins.

Elle salue par ailleurs le commentaire des articles relatif au paragraphe (5) qui renseigne que *« Le captage de sons est exclu… »* ainsi que *« Le recours à toute autre technique de détection automatique telle que la reconnaissance*

[25] Article 43bis paragraphe (12 alinéa 1° du projet de loi portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.
[26] *Ibidem,* alinéa 2°.
[27] *Ibidem,* alinéa 3°.
[28] *Ibidem,* alinéa 4°.
[29] *Ibidem,* paragraphe (5).

faciale est exclu ». En effet, le recours aux techniques de reconnaissance faciale dans le domaine répressif, actuellement en discussion au niveau européen, reste toujours très contestable d'un point de vue de la protection des données et de la vie privée. La CNPD est dès lors à se demander s'il ne faudrait pas exclure expressément dans le texte de loi tant le captage de sons que l'utilisation de techniques de détection automatique de reconnaissance faciale.

- Ad paragraphe (6) du nouvel article 43bis

En termes de proportionnalité du traitement de données et de garanties appropriées pour sauvegarder les droits et libertés fondamentaux des citoyens, la Commission nationale félicite également les auteurs du projet de loi d'avoir précisé que les caméras ne peuvent pas filmer l'intérieur des lieux d'accès privé, ni leurs entrées. Le texte prévoit encore l'obligation de recourir à des techniques de masquage irréversible lorsque la configuration des lieux ne permet pas d'exclure du champ de vision des caméras des entrées à des lieux d'accès privés. Si le règlement grand-ducal du 1er août 2007 ne contient pas une disposition similaire, il est vrai aussi que la Police grand-ducale utilise en pratique d'ores et déjà des techniques de masquage irréversible dans le cadre du système VISUPOL actuel.

Toutefois, à lire le paragraphe (6) du nouvel article 43bis, seules *« les images de l'intérieur des lieux d'accès privé, ni de façon spécifique, celles de leur entrées »* ne peuvent être visualisées. Par ailleurs, l'utilisation de procédés de masquage se limite aux *« entrées à des lieux d'accès privé »*. *A contrario*, l'intérieur d'un lieu privé peut être filmé et le recours à des procédés de masquage n'est pas obligatoire lorsque le lieu privé ne vise pas un accès ou une entrée. La CNPD estime dès lors nécessaire de préciser la disposition sous examen, afin de garantir que *ni l'intérieur, ni l'accès ou l'entrée d'un lieu privé* ne puissent être filmés et qu'en fonction de la configuration des lieux, tout intérieur, accès ou entrée d'un lieu privé soit masqué techniquement de manière irréversible.

- Ad paragraphe (7) du nouvel article 43bis

Le paragraphe (7) du nouvel article 43bis en projet précise que *« le public est informé de manière claire et permanente de l'existence du système de surveillance »*.

Dans la mesure où le paragraphe (8) du nouvel article 43bis renvoie à 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, il y a lieu de remarquer que l'article 11 paragraphe (1) de cette loi oblige d'ores et déjà tout responsable du traitement de prendre *« des mesures raisonnables pour fournir toute information, visée à l'article 12, ….., à la personne concernée d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par tout moyen approprié, y compris par voie électronique »*.

La Commission nationale ne voit dès lors pas de plus-value dans le texte du paragraphe (7) en question tout comme elle ne comprend pas l'emploi et la signification du terme *« permanent »* dans le contexte de cette disposition.

Pour ce qui concerne la mise en œuvre pratique par la Police grand-ducale pour informer les citoyens dans le cadre du système VISUPOL, la CNPD recommande vivement de suivre les lignes directrices élaborées par le Comité Européen de la Protection des Données, à savoir : *« Guidelines 3/2019 on processing of personal data through video devices, version 2.0, adopted on 29 January2020 ».*

- Ad paragraphe (8) du nouvel article 43bis

Le paragraphe (8) prévoit, entre autres, qu' *« un règlement grand-ducal détermine les mesures techniques et organisationnelles à mettre en œuvre par le responsable du traitement pour assurer la sécurité du traitement en application de l'article 28 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 et règle les modalités d'exercice du droit d'accès prévu à l'article 13 de la même loi ».*

La CNPD regrette qu'un projet de règlement grand-ducal n'ait pas été joint au projet de loi sous examen. Elle souligne cependant d'ores et déjà que lors de l'élaboration du règlement grand-ducal, une attention particulière devra être prêtée quant à la journalisation et au traçage des accès par les membres de la police. A ce titre, la CNPD rappelle qu'elle recommande régulièrement de conserver les logs pendant une période de 5 ans alors que ce délai correspond également au délai de prescription en matière délictuelle (p.ex. violation du secret professionnel). Notons que le règlement grand-ducal du 1er août 2007 ne prévoyait qu'une durée de conservation de 3 ans.

- Ad paragraphe (9) du nouvel article 43bis

Cette disposition règle la durée de conservation des images issues des caméras de surveillance. Le texte sous examen n'opère pas de changement par rapport au règlement grand-ducal du 1er août 2007, alors qu'il retient un délai de deux mois. La CNPD considère ce délai comme proportionné au regard des finalités poursuivis par le traitement de données.

- Ad paragraphe (10) du nouvel article 43bis

La Commission nationale accueille favorablement cette disposition, dans la mesure où le visionnage des images en temps réel est limité aux seuls membres de la Police désignés à cet effet par le directeur général de la Police.

Conclusion

La CNPD salue l'effort d'encadrer la mise en œuvre et l'exploitation de systèmes de vidéos surveillances par la Police grand-ducale et la modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale en y ajoutant un article 43bis à cette fin. Cet effort s'inscrit dans l'impératif de respecter le droit ainsi que la jurisprudence européenne.

Ainsi décidé à Esch-sur-Alzette en date du 28 février 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

ANNEXES

5

Avis relatif au projet de loi n°7467 portant transposition de certaines dispositions de 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/UE ; et portant 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 9 décembre 1976 relative à l'organisation du notariat ; c) la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice ; d) la loi modifiée du 10 août 1991 sur la profession d'avocat ; e) la loi modifiée du 10 juin 1999 portant organisation de la profession d'expert-comptable ; f) la loi modifiée du 23 juillet 2016 relative à la profession de l'audit.

(Délibération n°5/2020 du 28 février 2020)

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 ».*

Par courrier en date du 8 août 2019, Monsieur le Directeur du Trésor, pour le Ministre des Finances, a invité la Commission nationale à se prononcer au sujet du projet de loi n°7467 portant transposition de certaines dispositions de 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/UE ; et portant 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 9 décembre 1976 relative à l'organisation du notariat ; c) la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice ; d) la loi modifiée du 10 août 1991 sur la profession d'avocat ; e) la loi modifiée du 10 juin 1999 portant organisation de la profession d'expert-comptable ; f) la loi modifiée du 23 juillet 2016 relative à la profession de l'audit (ci-après « le projet de loi »).

Selon l'exposé des motifs, l'objectif du projet de loi est d'apporter à la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (ci-après « la loi de 2004 ») les adaptations nécessaires pour assurer la transposition de certaines dispositions de 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/UE (ci-après « la directive 2018/843 ») et d'assurer la mise en œuvre des recommandations du GAFI, notamment dans le cas où ces recommandations ne font pas l'objet de dispositions équivalentes dans 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/UE (ci-après « la directive 2015/849 »). Le projet de loi vise encore à compléter les pouvoirs des autorités de contrôles et des organismes d'autorégulation et à renforcer la coopération des autorités de contrôles avec leurs homologues étrangers.

L'article 5 de la directive 2015/849 permet aux États membres d'*« arrêter ou maintenir en vigueur, dans le domaine régi par la présente directive, des dispositions plus strictes pour prévenir le blanchiment de capitaux et le financement du terrorisme, dans les limites du droit de l'Union »*. La Cour de Justice dans un affaire concernant l'article correspondant de la directive 2005/60/CE du Parlement européen et du Conseil, du 26 octobre 2005, relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, telle que modifiée, a rappelé que la législation nationale adoptée doit, entre autres, être proportionnelle, ce qui nécessite une évaluation « *…du degré d'interférence des mesures de vigilance à l'égard de la clientèle qu'elle prévoit avec d'autres droits et intérêts protégés par le droit de l'Union, comme la protection des données à caractère personnel prévue à l'article 8 de la Charte …»*[30].

La CNPD rappelle que la protection des données à caractère personnel est un droit fondamental distinct et indépendant dans l'ordre juridique de l'UE, garanti par l'article 8 de la Charte des droits fondamentaux de l'Union européenne. La Cour de Justice a ainsi souligné qu'un acte est *« constitutif d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la charte puisqu'elle prévoit un traitement des données à caractère personnel »*[31]. Ce droit n'est pas absolu et peut être limité conformément à l'article 52, paragraphe 1 de la Charte, qui exige que la limitation soit prévue par la loi, respecte le contenu essentiel du droit à la protection des données et, dans le respect du principe de proportionnalité, qu'elle soit nécessaire et qu'elle répond effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

La Cour de justice a rappelé dans les affaires C-293/12 et C-594/12 Digital Rights que la lutte contre le terrorisme international et les crimes graves constitue une finalité d'intérêt général[32]. La CNPD souscrit à cet égard aux remarques du Contrôleur européen de la protection des données relatives à la proposition de directive 2015/849,

[30] Arrêt du 10 mars 2016, Safe Interenvios, C-235/14, ECLI:EU:C:2016:154, point 109 et également points 94 à 110, concernant l'article 5 de la directive 2005.
[31] Arrêt du 8 avril 2014, Digital Rights Ireland, affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, point 36; voir également Arrêt du 9 novembre 2010, Volker und Markus Schecke, affaires C-92/09 et C-93/09, ECLI:EU:C:2010:662, point 58. Voir encore Contrôleur européen de la protection des données, Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel (11 avril 2017).
[32] Arrêt du 8 avril 2014, Digital Rights Ireland, affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238, points 41-42.

qui a estimé plus précisément *« que les normes européennes en matière de protection des données n'ont pas d'équivalent à l'échelle internationale du GAFI, et que la recherche de cohérence entre les politiques de lutte contre le blanchiment de capitaux à l'échelle internationale ne devrait pas ignorer les exigences de l'Union européenne en matière de protection des données. Le CEPD rappelle que le droit d'un individu à la protection de ses données à caractère personnel est garanti par l'article 16 du TFUE et l'article 8 de la Charte des droits fondamentaux de l'Union européenne.*

Assurer la transparence des sources de paiements, des dépôts et virements de fonds afin de combattre le terrorisme et le blanchiment de capitaux est un intérêt légitime, mais cet objectif doit être poursuivi dans le respect des exigences en matière de protection des données.»[33].

Par ailleurs, le législateur européen a souligné l'importance du respect des droits fondamentaux lors de la mise en œuvre des recommandations du GAFI dans le considérant 43 de la directive 2015/849, qui énonce qu'*« il est essentiel que l'alignement de la présente directive sur les recommandations révisées du GAFI s'effectue dans le plein respect du droit de l'Union, en particulier en ce qui concerne le droit de l'Union en matière de protection des données et la protection des droits fondamentaux consacrée dans la charte »*.

Ainsi, dans la mesure où les auteurs du projet de loi vont au-delà de ce qui est prévu dans la directive 2015/849, ils doivent veiller à la conformité des dispositions avec la règlementation en matière de protection des données à caractère personnel. La CNPD ignore si une telle évaluation a été faite. Elle constate cependant qu'un grand nombre des modifications proposées ont un impact sur le droit à la protection des données et au respect de la vie privée des personnes physiques, dans la mesure où le nombre des traitements mis en œuvre et les données traitées tant par les professionnels que par les autorités compétentes et les organismes d'autorégulation accroîtront. De manière générale, les auteurs du projet de loi devraient analyser la nécessité et la proportionnalité des mesures proposées, d'autant plus si les mesures à mettre en œuvre en droit national n'ont pas fait l'objet d'une telle évaluation lors de leur élaboration.

La Commission nationale a déjà eu l'occasion de se prononcer sur la transposition des directives en matière de lutte contre le blanchiment et contre le financement du terrorisme dans ses avis n°51/2018 du 21 janvier 2018, n°485/2018 du 22 novembre 2018 et n°9/2019 du 17 janvier 2019. Elle souhaite ainsi profiter de l'occasion pour réitérer les remarques faites dans ces avis, notamment en ce qui concerne les catégories particulières de données, les données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté et les transferts de données vers des pays tiers par les professionnels.

Dans le présent avis, la Commission nationale se réfère aux articles de la version coordonnée de la directive 2015/849.

[33] Contrôleur européen de la protection des données, avis du 4 juillet 2013 sur une proposition de directive du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et une proposition de règlement du Parlement européen et du Conseil sur les informations accompagnant les virements de fonds, paragraphes 10-11.

I. Quant à la conservation des données à caractère personnel

La loi en projet sous avis vise dans son article 5, point 7, lettre c) à modifier l'article 3, paragraphe 6, lettre a) de la loi de 2004 relatif à la durée de conservation des données traitées par les professionnels en remplaçant les mots « peuvent conserver » par « conservent ».

Cette durée de conservation s'applique selon le nouvel alinéa 2 du paragraphe 6 de l'article 3 de la loi de 2004 également aux données accessibles par l'intermédiaire des mécanismes centralisés visés à l'article 32bis de la directive (UE) 2015/849.

Selon le commentaire des articles, cette modification a pour but *« d'appuyer le caractère obligatoire de la conservation pour une période supplémentaire de cinq ans lorsque cette conservation est nécessaire pour la mise en œuvre efficace des mesures internes de prévention ou de détection des actes de blanchiment ou de financement du terrorisme tel que prévu par l'article 40, paragraphe 1er, alinéa 2, de la directive (UE) 2015/849.»*[34].

Comme déjà soulevé dans l'avis de la CNPD n°51/2018 du 21 janvier 2018, l'article 40, paragraphe 1er, alinéa 2 de la directive 2015/849 fixe la durée de conservation des données collectées à 5 ans après la fin de la relation d'affaires ou de la transaction occasionnelle. Les États membres peuvent permettre ou exiger que les données soient conservées 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 »*.

Les auteurs du projet de loi n'ayant pas procédé à une analyse minutieuse de la nécessité et la proportionnalité de la prolongation de la durée de conservation, la CNPD n'est pas en mesure d'apprécier la nécessité et la proportionnalité de la disposition en question. Elle se réfère pour le surplus à ses remarques faites dans son avis n°51/2018 du 21 janvier 2018.

II. Quant aux droits des personnes concernées

La CNPD prend note de l'alignement des alinéas 3 et 4 de l'article 3, paragraphe 6bis de la loi de 2004, telle que modifiée par le projet de loi, sur le RGPD. Elle remarque que les auteurs du projet de loi ont précisé le champ d'application de la limitation du droit d'accès de la personne concernée.

Ainsi, conformément à l'article modifié, le droit d'accès prévu à l'article 15 du RGPD peut être limité *« en application de l'article 5, paragraphe (5), alinéa 1 »*, à savoir lorsque *« des informations sont, seront ou ont été communiquées ou fournies aux autorités en application des paragraphes (1), (1bis), (2) et (3) [de l'article 5] ou qu'une enquête*

[34] Projet de loi n°7467, Commentaire des articles, page 51.

de la cellule de renseignement financier sur le blanchiment ou le financement du terrorisme est en cours ou pourrait être ouverte » (article 5, paragraphe 5, alinéa 1er).

La disposition sous revue constitue une limitation des droits des personnes concernées au sens de l'article 23 du RGPD, selon lequel la portée du droit d'accès peut être limitée par le droit de l'Union ou d'un État membre, lorsque cette limitation respecte l'essence des libertés et droits fondamentaux et constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des objectifs prévus limitativement à l'article 23, paragraphe 1er du RGPD. Les mesures législatives doivent prévoir des dispositions spécifiques relatives, au moins, aux éléments visés au paragraphe 2 de l'article en question, y compris des dispositions relatives à la formulation des finalités ou catégories de finalités, les catégories de données à caractère personnel concernées et l'étendue des limitations.

Dans un souci de sécurité juridique et afin de délimiter avec suffisamment de précision les cas dans lesquels le droit d'accès des personnes concernées pourrait être limité, le projet de loi devrait être précisé afin de satisfaire aux exigences de l'article 23 du RGPD, en indiquant, entre autres, les conditions précises s'appliquant à la limitation du droit de la personne concernée. La CNPD se réfère à cet égard à ses avis et aux avis du Conseil d'État relatifs au projets de loi n°7250 et n°7373. Dans le cas d'espèce, la Commission nationale s'interroge, notamment, sur la possibilité de limiter le droit d'accès, dans l'hypothèse où une enquête ne serait pas ouverte mais « pourrait l'être » par la CRF. En effet, la disposition ne précise pas quand et comment un responsable du traitement-professionnel pourrait estimer qu'une enquête pourrait être ouverte par la CRF.

A l'instar de son avis n°51/2018 du 21 janvier 2018, la CNPD insiste encore sur la nécessité de prévoir un droit d'accès indirect si le droit d'accès de la personne concernée a été limité.

III. <u>Quant à la coopération entre la CRF, les autorités de contrôle et les organismes d'autorégulation</u>

a. Le principe de limitation des finalités

i. <u>Considérations générales</u>

Conformément à l'article 8, paragraphe 2 de la Charte des droits fondamentaux, les données à caractère personnel doivent être traitées loyalement et à des fins déterminées. Ainsi, conformément au principe de limitation des finalités, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Ce principe s'applique aux traitements de données effectués par les autorités, y compris dans le cadre de la coopération nationale et internationale.

La CNPD souscrit entièrement à l'avis du Contrôleur européen de la protection de données sur la proposition de la Commission européenne modifiant la directive (UE) 2015/849 et la directive 2009/101/CE que le principe

de limitation des finalités est particulièrement important *« en ce qui concerne l'ingérence de l'ordre public dans la protection des données à caractère personnel, car la proportionnalité de leur traitement devra être évaluée en fonction de l'objectif politique défini par le législateur.*

À cet égard, nous considérons que des instruments législatifs permettant le traitement multiple et/ou simultané de données à caractère personnel par différents responsables du traitement des données et à des fins incompatibles, sans préciser dans quel but chaque traitement de données est effectué, risque de causer une très grande confusion en ce qui concerne l'application du principe de proportionnalité.

Dans les cas pour lesquels les finalités du traitement des données sont définies par des termes généraux ou vagues, ou pour lesquels les divers responsables du traitement des données ont une relation complètement différente avec la finalité poursuivie tant sur le plan de la structure ou des ressources que de la capacité de chaque responsable à respecter les règles dans certaines circonstances données, le principe de limitation des finalités est compromis formellement et de façon substantielle et, par conséquent, le principe de proportionnalité ne sera pas non plus dûment appliqué »[35].

Il convient donc d'indiquer avec précision les finalités des traitements entrepris par les autorités.

Pour satisfaire à l'exigence de spécificité, la finalité doit être clairement et pleinement identifiée afin de déterminer quel traitement est ou n'est pas inclus dans la finalité spécifiée et de permettre l'évaluation du respect de la loi et l'application de garanties en matière de protection des données. Les finalités doivent encore être explicites, c'est-à-dire claires, expliquées ou exprimées sous une forme ou une autre afin de s'assurer que toutes les personnes concernées ont la même compréhension univoque des finalités du traitement, indépendamment de toute diversité culturelle ou linguistique[36].

Par ailleurs, le fondement du traitement devrait être clair et précis 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.[37]

ii. <u>Obligation de coopération avec la CRF, les autorités de contrôle et les organismes d'autorégulation (articles 5 et 9-1 de la loi de 2004, telle que modifiée par le projet de loi)</u>

Selon le nouvel article 5, paragraphe 1er de la loi de 2004, les professionnels, leurs dirigeants et employés doivent coopérer avec *« les autorités luxembourgeoises responsables de la lutte contre le blanchiment et contre le financement du terrorisme et les organismes d'autorégulation, en particulier dans le cadre de l'exercice de leurs pouvoirs de surveillance respectifs conférés par les articles 8-2 et 8-2bis ».*

[35] Contrôleur européen de la protection des données, Avis du 2 février 2017 sur la proposition de la Commission modifiant la directive (UE) 2015/849 et la directive 2009/101/CE, paragraphes 20-23.
[36] Groupe de travail « Article 29 », Avis 03/2013 sur la limitation de la finalité (WP203), page 38.
[37] Considérant 41 du RGPD (« 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 ») et considérant 33 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 (« ce droit d'un État membre, cette base juridique ou cette mesure législative devrait être clair et précis et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice et de la Cour européenne des droits de l'Homme. »)

La CNPD s'interroge sur la portée de cette disposition. En effet, vu la référence aux pouvoirs des autorités responsables et des organismes d'autorégulation conférés par les articles 8-2 et 8-2bis, faut-il comprendre que l'article 5, paragraphe 1er de la loi de 2004 concerne uniquement les autorités de contrôle et les organismes d'autorégulation ?

Dans un souci de sécurité juridique, la Commission nationale estime nécessaire de préciser davantage cette disposition, notamment en précisant les entités couvertes par la notion d'*« autorités luxembourgeoises responsables de la lutte contre le blanchiment et contre le financement du terrorisme »*. Par ailleurs et en tenant compte de ce qui précède concernant la limitation des finalités, la CNPD estime nécessaire de supprimer les mots « en particulier » et de préciser le cadre dans lequel les professionnels doivent coopérer avec les autorités en question.

En outre, il convient de rappeler à cet égard l'article 5, paragraphe 2 de la loi de 2004, qui précise que *« les informations et pièces fournies aux autorités, autres que les autorités judiciaires, en application des paragraphes (1) et (1bis) peuvent être utilisées uniquement à des fins de lutte contre le blanchiment ou contre le financement du terrorisme. »* En accord avec la modification de l'article 5, paragraphe 1er, le paragraphe 2 devrait être modifié afin d'y intégrer les organismes d'autorégulation.

En ce qui concerne l'article 9-1 de la loi de 2004, tel qu'il résulte du projet de loi, celui-ci prévoit que la CRF, les autorités de contrôle et les organismes d'autorégulation coopèrent étroitement entre eux. Quant à la forme et les finalités de la coopération, l'alinéa 2 précise que *« 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. »*

Aucune information n'est fournie ni sur la forme, ni sur les finalités de la coopération entre la CRF, les autorités de contrôle et les organismes d'autorégulation. Plus précisément, le projet de loi n'indique pas si les organismes d'autorégulation pourraient échanger des données à caractère personnel avec la CRF et les autorités de contrôle. En tenant compte de l'alinéa 2 de l'article 9-1 cité ci-avant, il semble dès lors qu'il n'y aura pas d'échange de données entre les organismes d'autorégulation, d'une part, et la CRF et les autorités de contrôle, d'autre part.

Si malgré ceci les organismes d'autorégulation pourraient être amenés à échanger des données avec la CRF et les autorités de contrôle, le Conseil d'État a souligné à plusieurs reprises que la communication de données à des tiers peut constituer une ingérence dans la vie privée[38] et constitue ainsi en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Il faut donc que les points essentiels soient fixés par la loi.

[38] Avis du Conseil d'État du 21 novembre 2017 relatif au projet de loi n°7182, doc. parl. 7182/02, page 7. Avis du Conseil d'État du 7 juin 2016 relatif au projet de loi n°6975, page 4.

Ainsi, en tenant compte de ce qui précède et si la CRF, les autorités de contrôle et les organismes d'autorégulation seraient amenés à échanger des données à caractère personnel, le projet de loi devrait encadrer la coopération de tous les responsables du traitement en question, en précisant la forme et la finalité de cette coopération pour tous les responsables du traitement, y compris les organismes d'autorégulation.

iii. Coopération nationale entre la CSSF et la CAA agissant aux fins de la lutte contre le blanchiment et contre le financement du terrorisme et aux fins de la surveillance prudentielle des établissements de crédit et des établissements financiers ou de la surveillance des marchés financiers (article 9-1bis de la loi de 2004, telle que modifiée par le projet de loi)

L'article 1er, paragraphe 37 de la directive 2018/843 introduit des dispositions spécifiques concernant l'échange d'informations entre les autorités compétentes en insérant un nouvel article 57bis dans la directive 2015/849. Conformément à cet article, les autorités compétentes chargées de la surveillance des établissements de crédit et des établissements financiers au sein d'un État membre et dans différents États membres conformément à la directive ou à d'autres actes législatifs relatifs à la surveillance des établissements de crédit et des établissements financiers peuvent échanger des données.

Le paragraphe 3 de l'article 57*bis* de la directive 2015/849 énumère les finalités aux fins desquelles les données échangées peuvent être utilisées. Il s'agit entres autres de *« … l'accomplissement des devoirs qui leur incombent en vertu de la présente directive ou d'autres actes législatifs dans le domaine de la lutte contre le blanchiment de capitaux et le financement du terrorisme, de la réglementation prudentielle et de la surveillance des établissements de crédit et des établissements financiers, notamment l'imposition de sanctions » et « dans le cadre de procédures juridictionnelles engagées en vertu de dispositions spéciales prévues par le droit de l'Union dans le domaine de la présente directive ou dans celui de la réglementation prudentielle et de la surveillance des établissements de crédit et des établissements financiers. ».*

Selon le commentaire des articles du projet de loi, l'article 57bis de la directive 2015/849 serait transposé par l'article 9-1bis de la loi de 2004, telle que modifiée par le projet de loi, selon lequel que la CSSF et le CAA peuvent échanger des données *« (…) aux fins de la lutte contre le blanchiment et contre le financement du terrorisme ainsi qu'aux fins d'autres actes législatifs relatifs à la règlementation et à la surveillance prudentielle des établissements de crédit et des établissements financiers ou relatifs à la surveillance des marchés financiers »*[39]*. A l'instar de la directive, le paragraphe 3 énonce les finalités aux fins desquelles les données peuvent être échangées, en se référant également à « …d'autres actes législatifs dans le domaine … de la réglementation et de la surveillance prudentielle des établissements de crédit et des établissements financiers ainsi que de la surveillance des marchés financiers. ».*

Le commentaire des articles précise que *« [c]e nouvel article tient compte du fait que les informations à caractère prudentiel relatives aux établissements de crédit et aux établissements financiers, telles que les données relatives*

[39] Article 9-1bis, paragraphe 1er de la loi de 2004, telle que modifiée par le projet de loi.

à l'honorabilité des directeurs et des actionnaires, aux mécanismes de contrôle interne, à la gouvernance ou à la conformité et à la gestion des risques, sont souvent indispensables à la surveillance appropriée de ces institutions en termes de lutte contre le blanchiment et le financement du terrorisme. De la même manière, les informations sur la lutte contre le blanchiment et le financement du terrorisme sont également importantes pour la surveillance prudentielle de ces institutions. C'est dans cette optique que la directive 2018/843 vise à fournir un cadre juridique en élargissant l'échange d'informations confidentielles et la coopération entre autorités compétentes en matière de lutte contre le blanchiment et le financement du terrorisme ainsi qu'en matière de surveillance prudentielle des établissements de crédit et des établissements financiers. Dans tous les cas, les informations échangées devront présenter un élément pertinent en matière de lutte contre le blanchiment et le financement du terrorisme. »[40]

Au vu de ce qui précède et en tenant compte du principe de limitation des finalités, la Commission nationale considère que la finalité telle qu'actuellement rédigée, à savoir *« (…) aux fins d'autres actes législatifs relatifs à la règlementation et à la surveillance prudentielle des établissements de crédit et des établissements financiers ou relatifs à la surveillance des marchés financiers »* est formulée de manière trop vague. Elle estime dès lors nécessaire de préciser les actes législatifs sur base desquels la CSSF et le CAA pourraient échanger des données à caractère personnel. Par ailleurs, afin d'assurer le principe de limitation des finalités et pour éviter toute ambiguïté, la précision dans le commentaire des articles que les informations échangées doivent être nécessaire en matière de lutte contre le blanchiment et le financement du terrorisme devrait figurer dans le corps même du texte.

iv. La coopération internationale des autorités de contrôle avec leurs autorités homologues étrangères (article 9-2*bis* de la loi de 2004, telle que modifiée par le projet de loi) et la coopération internationale de la CSSF et du CAA avec leurs autorités homologues étrangères (article 9-2quater de la loi de 2004, telle que modifiée par le projet de loi)

Les articles 9-2*bis* et 9-2*ter* de la loi de 2004, telle que modifiée par le projet de loi, visent à instaurer un cadre juridique pour la coopération des autorités de contrôle avec leurs autorités homologues étrangères (article 9-2*bis*), respectivement pour la coopération de la CSSF et du CAA avec leurs autorités homologues étrangères agissant aux fins de la lutte contre le blanchiment et contre le financement du terrorisme et aux fins de la surveillance prudentielle des établissements de crédit et des établissements financiers ou de la surveillance des marchés financiers (article 9-2*quater*).

La CNPD note que le projet de loi sous avis ne distingue pas entre la coopération européenne et la coopération internationale avec des autorités des pays tiers, tel qu'il est le cas dans la directive 2015/849. En effet, la directive encadre la coopération entre les autorités des États membres, par exemple en fixant les cas dans lesquels les autorités nationales peuvent rejeter une demande d'assistance. Les conditions entourant la coopération européenne ne sont pas imposées par la directive 2015/849 pour la coopération avec des autorités avec des pays tiers, mais sont introduites par le projet de loi sous avis afin d'encadrer la coopération avec les autorités des pays tiers. Ainsi,

[40] AProjet de loi n°7467, Commentaires des articles, pages 65-66.

les autorités nationales ne pourraient à l'avenir rejeter des demandes des autorités des pays tiers que conformément aux critères prévus à l'article 9-2*ter*. La Commission nationale remarque qu'une demande de coopération pourrait être refusée, si *« l'autorité homologue requérante n'est pas en mesure de protéger efficacement ces informations »* (articles 9-2*ter,* lettre b) et 9-2*quater,* paragraphe 4 de la loi de 2004, telle que modifiée par le projet de loi). Afin d'assurer la protection des données lors de la coopération, l'évaluation de la protection des informations devrait également inclure une évaluation du niveau de protection des données à caractère personnel.

En ce qui concerne les finalités des échanges, la CNPD renvoie à ses observations faites au point III.a.i. et iii. ci-dessus concernant la précision des finalités. En outre, le paragraphe 6 de l'article 9-2*bis* et le paragraphe 6 de l'article 9-2*quater* de la loi de 2004, telle que modifiée par le projet de loi, restreint l'utilisation des données reçues par les autorités nationales par des autorités étrangères. Dans la mesure où la liste des finalités constitue une liste limitative, il faudrait supprimer les mots « en particulier » de la disposition.

En outre, la Commission nationale s'interroge sur la portée de cette coopération, entres autres en ce qui concerne les données pouvant être transmises. Par exemple, les autorités doivent transmettre *« toute information requise »* (articles 9-2bis, paragraphe 2, alinéa 1er et 9-2*quater,* paragraphe 2, alinéa 1er de la loi de 2004, telle que modifiée par le projet de loi). Le paragraphe 9 du nouvel article 9-2*quater* de la loi de 2004 prévoit une liste des « types d'informations » pouvant être échangés par la CSSF et le CAA dans le cadre de la coopération internationale avec leurs autorités homologues étrangères, en particulier les autorités homologues partageant une responsabilité commune vis-à-vis des établissements de crédit ou des établissements financiers qui opèrent au sein du même groupe.

Par ailleurs, les autorités doivent prendre *« sans délais les mesures nécessaires pour recueillir les informations sollicitées en faisant usage des pouvoirs dont elle dispose en vertu des pouvoirs qui lui sont conférés par la loi »* (articles 9-2*bis,* paragraphe 2, alinéa 3 et 9-2*quater,* paragraphe 2, alinéa 2 de la loi de 2004, telle que modifiée par le projet de loi). Il n'est pas clair en vertu de quelle loi les autorités pourraient recueillir les informations sollicitées.

En tenant compte également du fait que les finalités aux fins desquelles les données pourraient être échangées ne sont pas indiquées avec suffisamment de précision (voir ci-avant), la Commission nationale estime que la formulation employée dans l'article 9-2*bis* et 9-2*quater* est trop vague et estime nécessaire d'encadrer davantage la coopération des autorités, notamment en fixant avec plus de précision les données qui pourraient être échangées, les sources des données ainsi que les garanties entourant ces échanges. Il faudrait également remplacer le mot « requise » par le mot « nécessaire ».

b. La confidentialité des données échangées par les autorités de contrôle

Quant à la confidentialité, la CNPD note que les articles 9-2*bis,* paragraphe 7 et 9-2*quater,* paragraphe 8 de la loi de 2004, telle que modifiée par le projet de loi, prévoient que les autorités *« assurent un degré de confidentialité*

approprié à toute demande de coopération et aux informations échangées, de manière à protéger l'intégrité des enquêtes ou des recherches d'informations, dans le respect des obligations des deux parties en matière de respect de la vie privée et de protection des données. ». La CNPD rappelle que les autorités doivent, en tout état de cause, agir en conformité avec la législation en matière de protection des données et vie privée et que l'assurance d'un « degré de confidentialité approprié » ne peut en aucun cas conduire à une réduction du niveau de protection offert par la législation en matière de protection des données.

c. Les transferts de données vers des pays tiers

La CNPD rappelle que tout transfert de données à caractère personnel par la CRF, les autorités de contrôle et les organismes d'autorégulation vers des pays tiers, à savoir en dehors de l'Espace Economique Européen, doit être conforme au chapitre 3 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, respectivement au chapitre V du RGPD.

Quant au RGPD, il ressort de l'article 44 du RGPD que toutes les dispositions du chapitre V doivent être appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le RGPD ne soit pas compromis. Ainsi, en l'absence de décision d'adéquation au sens de l'article 45 du RGPD ou de garanties appropriées au sens de l'article 46 du RGPD, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu que dans les cas limitativement énumérés par l'article 49 du RGPD. En ce qui concerne le recours à l'article 49 du RGPD, la CNPD renvoie aux lignes directrices 2/2018 du Comité européen de la protection des données 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679. A l'instar de ces lignes directrices, la CNPD tient à souligner que ces dérogations *« doivent être interprétées de manière à ne pas contredire la nature même des dérogations, qui sont des exceptions à la règle qui veut que les données à caractère personnel ne peuvent être transférées vers un pays tiers à moins que ce pays offre un niveau adéquat de protection des données ou que des garanties appropriées soient mises en place »*[41].

IV. <u>Quant aux pouvoirs des autorités de contrôle et des organismes d'autorégulation</u>

La Commission nationale a déjà eu l'occasion d'aviser les pouvoirs des autorités de contrôle dans son avis n°51/2018 du 21 janvier 2018.

Elle note que l'article 8-2bis de la loi de 2004, telle que modifiée par le projet de loi vise à accorder des nouveaux pouvoirs aux organes compétents des organismes d'autorégulation, 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 d'exiger la communication des enregistrement téléphoniques, des communications électroniques ou des enregistrement de données relatives

[41] Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679 du Comité européen de la protection des données, p. 5.

aux trafic détenues par des personnes soumises à leur pouvoir de surveillance respectif[42]. Selon le commentaire des articles, les articles visent à aligner les pouvoirs de surveillance des organismes d'autorégulation sur ceux des autorités de contrôle[43].

Selon l'article 48, paragraphes 2 et 9 de la directive 2015/849, lorsque les organismes d'autorégulation sont investis de la mission de surveillance prévue au paragraphe 1er dudit article, les États membres doivent veiller à ce qu'ils disposent *« des pouvoirs appropriés, dont le pouvoir d'exiger la production de toute information pertinente pour contrôler le respect des obligations et le pouvoir d'effectuer des vérifications… »*. L'article 61 de la directive dispose que les autorités compétentes et les organismes d'autorégulation doivent mettre en place des mécanismes de « whistleblowing ». Or, selon l'article 60 de la directive 2015/849, uniquement les autorités compétentes doivent publier les décisions n'ayant fait l'objet d'aucun recours et instituant une sanction ou une mesure administrative en raison d'une infraction.

La CNPD s'interroge donc sur la proportionnalité et la nécessité de l'introduction de tels pouvoirs et missions pour les organismes d'autorégulation. Etant donné que l'article 48, paragraphe 3 de la directive 2015/849 prévoit que *« Les autorités compétentes disposent de pouvoirs renforcés en matière de surveillance en ce qui concerne les établissements de crédit, les établissements financiers et les prestataires de services de jeux d'argent et de hasard. »*, il semble qu'il n'est pas envisagé que toutes les autorités compétentes et les organismes d'autorégulation disposent des pouvoirs identiques. La CNPD recommande dès lors aux auteurs du projet de loi d'analyser s'il est nécessaire et proportionnel de conférer aux organismes d'autorégulation des pouvoirs identiques à ceux conférés aux autorités de contrôle.

Ainsi décidé à Esch-sur-Alzette en date du 28 février 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

[42] Nouvel article 8-2bis de la loi de 2004, telle que modifiée par le projet de loi.
[43] Projet de loi n°7467, Commentaires des articles, pages 59-61.

ANNEXES

5

Avis relatif au projet de loi n°7216B 1) portant transposition de : a) l'article 31 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 ; et b) l'article 1er, point 16, de 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/UE ; 2) portant modification de la loi modifiée du 27 juillet 2003 relative au trust et aux contrats fiduciaires ; et 3) portant abrogation de la loi du 10 août 2018 relative aux informations à obtenir et à conserver par les fiduciaires et portant transposition de l'article 31 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.

(Délibération n° 6/2020 du 28 février 2020)

Conformément à l'article 57, paragraphe 1er, lettre (c) 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, 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 ».*

Par courrier en date du 11 octobre 2019, Monsieur le Ministre des Finances a invité la Commission nationale à se prononcer sur les amendements gouvernementaux au projet de loi n°7216B instituant un registre des fiducies et portant transposition de l'article 31 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 »).

Une partie de l'article 31 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 (ci-après « la directive 2015/849 »), telle que modifiée 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/UE (ci-après « la directive 2018/843 ») a été transposée par la loi du 10 août 2018 relative aux informations à obtenir et à conserver par les fiduciaires (ci-après « la loi du 10 août 2018 »). Dès lors, afin de ne pas disposer de deux lois distinctes au niveau national transposant un même article de la directive 2015/849, les auteurs proposent d'abroger la loi du 10 août 2018 et d'insérer les dispositions auparavant contenues dans la loi du 10 août 2018 dans ce projet de loi tout en assurant que les modifications apportées par la directive 2018/843 à ces dispositions soient répercutées dans le présent projet de loi n°7216B. Les auteurs visent également à tenir compte des principes établis par la recommandation 25 du Groupe d'action financière (ci-après « GAFI »).

Le projet de loi comporte ainsi deux volets. Premièrement, le projet de loi prévoit l'obligation pour les fiduciaires et les trustees d'obtenir et de conserver des données relatives aux bénéficiaires effectifs ainsi qu'à d'autres personnes spécifiées dans le projet de loi. Deuxièmement, le projet de loi vise à instaurer un registre des fiducies et des trusts (ci-après désigné « le registre ») tenu par l'Administration de l'enregistrement, des domaines et de la TVA (ci-après désignée « l'AED ») dans lequel les fiduciaires et les trustees devront faire inscrire certaines données qu'ils sont obligés de collecter en vertu de la loi en projet.

La CNPD a déjà eu l'occasion de se prononcer sur la transposition des directives en matière de lutte contre le blanchiment et contre le financement du terrorisme dans ses avis n°51/2018 du 21 janvier 2018, n°485/2018 du 22 novembre 2018 et n°9/2019 du 17 janvier 2019.

Le présent avis de la Commission nationale tiendra compte des amendements gouvernementaux en se basant sur la numérotation du texte coordonné. Elle se réfère également aux articles de la version coordonnée de la directive 2015/849.

A titre liminaire, la CNPD note que le projet de loi utilise la notion de « personne concernée » dans le cadre des informations relatives aux personnes physiques et aux personnes morales devant être inscrites dans le registre. Afin d'éviter une quelconque confusion avec la notion de « personne concernée » relative à une « personne physique » relevant de la règlementation en matière de protection des données, la CNPD recommande aux auteurs du projet de loi d'utiliser une terminologie différente pour ce qui est des « personnes morales ».

ANNEXES

5

I. <u>Quant aux données traitées par les trustees et les fiduciaires (articles 2 et 3)</u>

La collecte de données par les trustees et les fiduciaires est principalement régie par les articles 2 et 3 du projet de loi. Or, ces articles ne définissent pas clairement les données devant être collectées par les fiduciaires et les trustees.

L'article 31, paragraphe 1er, alinéa 2 de la directive 2015/849 concernant les données à collecter par les fiduciaires et les trustees prévoit que chaque État membre exige que les « *fiduciaires/trustees de toute fiducie expresse/de tout trust exprès administré dans ledit État membre obtiennent et conservent des informations adéquates, exactes et actuelles sur les bénéficiaires effectifs de la fiducie/du trust. Ces informations comprennent l'identité (a) du ou des constituants, (b) du ou des fiduciaires/trustees, (c) du ou des protecteurs (le cas échéant), (d) des bénéficiaires ou de la catégorie de bénéficiaires, et (e) de toute autre personne physique exerçant un contrôle effectif sur la fiducie/le trust.* ». Ces informations incluent, au moins, le nom, le mois et l'année de naissance, le pays de résidence et la nationalité du bénéficiaire effectif, ainsi que la nature et l'étendue des intérêts effectifs détenus (article 31, paragraphe 4, alinéa 2 de la directive 2015/849).

En transposant cet article, l'article 2, paragraphe 1er du projet de loi impose aux trustees et aux fiduciaires d'obtenir et de conserver « *des informations* » sur les bénéficiaires effectifs de tout trust exprès administré au Luxembourg ou de toute fiducie pour laquelle ils occupent la fonction de trustee ou de fiduciaire. Ces informations « *comprennent* » l'identité du ou des constituants, du ou des trustees ou fiduciaires, du ou des protecteurs (le cas échéant), des bénéficiaires ou de la catégorie de bénéficiaires ainsi que de toute autre personne physique exerçant un contrôle effectif sur le trust ou la fiducie. Alors que le projet de loi et le commentaire des articles n'y fait pas référence, le commentaire des articles du projet de loi n°7216 précisait que *« les informations à obtenir et à conserver incluent les informations à inscrire dans le Registre des fiducies conformément à l'article 14, paragraphe 2, de la loi en projet »*[44].

En outre, les trustees et les fiduciaires doivent transmettre aux professionnels « *des données relatives aux avoirs du trust et le patrimoine des fiducies détenus ou gérés dans le cadre de la relation d'affaires* » (article 6, paragraphe 2 du projet de loi). Le commentaire des articles n'explique pas quels types de données sont couverts par cette obligation.

Par ailleurs, selon l'article 8, paragraphes 5 et 6 du projet de loi, les fiduciaires et les trustees, respectivement les professionnels, fournissent, sur demande, « *toute information qu'ils détiennent sur toute fiducie ou tout trust* » aux personnes visées à l'article 1er, paragraphe 1er, point 1er, lettres a) à c) et point 2 du projet de loi, à savoir le procureur général d'État, les procureurs d'État ainsi que les membres de leurs parquets, les juges d'instruction, la Cellule de renseignement financier (ci-après « la CRF ») et les autorités de contrôle.

En sus des données indiquées ci-avant, il semble que les trustees et les fiduciaires doivent également collecter et, le cas échéant, transmettre à l'AED des pièces justificatives (quelles qu'elles soient) auxquelles le projet de loi fait référence dans son article 18.

[44] Projet de loi n°7216, doc. parl n° 7216/00, p. 11.

L'article 3, en son paragraphe 1er dispose que *« les trustees des trusts exprès administrés au Luxembourg et les fiduciaires obtiennent et conservent des informations élémentaires sur les autres agents réglementés et prestataires de services du trust ou de la fiducie, y compris les conseillers en investissement ou gestionnaires d'investissement, les comptables et les conseillers fiscaux. »*. Les personnes visées sont obligées de fournir aux trustees et fiduciaires toutes les informations nécessaires pour que ceux-ci puissent satisfaire aux obligations leur incombant en vertu du paragraphe 1er (paragraphe 2).

La CNPD note tout d'abord que l'article 3 du projet de loi, contrairement à l'article 2, ne figure pas à l'article 31 de la directive 2015/849, mais est tiré exclusivement de la recommandation 25 du GAFI. Les auteurs des amendements ne fournissant pas d'explications quant à une éventuelle analyse de la nécessité et de la proportionnalité qui aurait été effectuée au sujet d'une telle obligation, de sorte que la CNPD n'est pas en mesure d'analyser la conformité d'une telle disposition avec la règlementation en matière de protection des données. Elle tient néanmoins à souligner que la formulation selon laquelle les trustees et les fiduciaires doivent collecter des informations relatives aux *« autres agents réglementés et prestataires de services du trust ou de la fiducie, y compris les conseillers en investissement ou gestionnaires d'investissement, les comptables et les conseillers fiscaux »* n'est pas formulée de manière suffisamment précise pour permettre aux trustees, aux fiduciaires et aux personnes visées à l'article d'identifier avec précision les personnes concernées visées. S'y ajoute que l'article prévoit que les trustees et les fiduciaires doivent collecter des « informations élémentaires », sans pour autant préciser ces « informations élémentaires ». Par ailleurs, contrairement à l'article 2, paragraphe 2, l'article 3 n'exige pas que les données soient « adéquates », ce qui contribue au caractère vague de cette disposition.

L'article 5, paragraphe 1, lettre (c) du RGPD énonce que 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). Afin d'empêcher une collecte de données indifférenciée et arbitraire, il conviendrait d'analyser la nécessité et la proportionnalité des données devant être traitées par les trustees et les fiduciaires dans le cadre du présent projet de loi, y compris la nécessité et la proportionnalité de l'article 3 du projet de loi. Par ailleurs, à l'instar de la recommandation du Contrôleur européen de la protection de données (ci-après « le CEPD ») émise dans son avis sur le projet de directive n°2015/849[45], la CNPD estime nécessaire d'amender le projet de loi afin d'y indiquer les catégories de données, qui doivent être obtenues et conservées par les trustees et les fiduciaires. Si les auteurs du projet de loi estiment nécessaires d'imposer une collecte des pièces justificatives, ils devraient également préciser les pièces justificatives en question.

La Commission nationale relève encore que les notions de *« catégorie de bénéficiaires effectifs »* et *« l'étendue des intérêts effectifs détenus »* ne sont pas définies dans le projet de loi. Afin de définir clairement les informations devant être conservées et de respecter ainsi le principe de minimisation des données, elle suggère dès lors de clarifier ces notions.

[45] Avis du Contrôleur européen de la protection des données du 4 juillet 2013 sur une proposition de directive du Parlement européen et du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et une proposition de règlement du Parlement européen et du Conseil sur les informations accompagnant les virements de fonds, points 83-84.

II. <u>Quant à la transmission des données détenues par les fiduciaires et les trustees aux autorités nationales, aux organismes d'autorégulation et aux professionnels (article 5 et 6)</u>

L'article 5, paragraphe 1er et 2 du projet de loi dispose que les fiduciaires et les trustees doivent fournir aux autorités nationales aux fins de leurs missions et aux organismes d'autorégulation aux fins de leurs missions en vertu de la présente loi et de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme, sur demande, *« les informations visées aux articles 2 et 3, ainsi que, le cas échéant, le numéro d'immatriculation unique visé à l'article 13, paragraphe 3, ou une attestation apportant la preuve de l'enregistrement dans un registre équivalent mis en place par un autre État membre ou un extrait des informations sur les bénéficiaires effectifs conservées dans un tel registre »*. Les « autorités nationales » sont toutes les autorités, administrations et entités indiquées à l'article 1er, paragraphe 1er, point 1er du projet de loi.

Cet article vise à transposer l'article 31, paragraphe 3 de la directive 2015/849[46], qui prévoit que *« Les États membres exigent que les autorités compétentes et les CRF puissent accéder en temps utile aux informations visées au paragraphe 1 »*.

Quant aux finalités de l'accès aux données, le commentaire des articles du projet de loi explique que ce paragraphe vise non seulement à transposer la directive 2018/843, mais encore l'article 22, paragraphe 1bis de la directive 2011/16/UE du Conseil du 15 février 2011 relative à la coopération administrative dans le domaine fiscal[47].

Afin d'assurer la conformité avec la législation en matière de protection de données, le texte du projet de loi devrait préciser les missions des autorités pouvant accéder aux données et identifier clairement les finalités de l'accès.

En effet, l'article 8, paragraphe 2 de la Charte des droits fondamentaux exige que les données à caractère personnel soient traitées loyalement et à des fins déterminées. Ainsi, conformément au principe de la limitation des finalités, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne doivent pas être traitées d'une manière incompatible avec ces finalités.

Pour satisfaire à l'exigence de spécificité, la finalité doit être clairement et pleinement identifiée afin de déterminer quel traitement est ou n'est pas inclus dans la finalité spécifiée et permettre l'évaluation du respect de la loi et l'application des garanties en matière de protection des données[48]. Les finalités doivent encore être explicites, c'est-à-dire claires, expliquées ou exprimées sous une forme ou une autre afin de s'assurer que toutes les personnes concernées ont la même compréhension univoque des finalités du traitement, indépendamment de toute diversité culturelle ou linguistique[49].

La CNPD se rallie à cet égard à l'avis du CEPD sur la proposition de la Commission européenne modifiant la directive (UE) 2015/849 et la directive 2009/101/CE, selon lequel *« À cet égard, nous considérons que des*

[46] Projet de loi n°7216B, doc. parl n°7216B/03, Commentaire des articles, p. 11.
[47] Projet de loi n°7216B, doc. parl n°7216B/03, Commentaire des articles, p. 11.
[48] Groupe de travail « Article 29 », Avis 03/2013 sur la limitation de la finalité (WP203), page 39.
[49] Groupe de travail « Article 29 », Avis 03/2013 sur la limitation de la finalité (WP203), page 39.

instruments législatifs permettant le traitement multiple et/ou simultané de données à caractère personnel par différents responsables du traitement des données et à des fins incompatibles, sans préciser dans quel but chaque traitement de données est effectué, risque de causer une très grande confusion en ce qui concerne l'application du principe de proportionnalité.

Dans les cas pour lesquels les finalités du traitement des données sont définies par des termes généraux ou vagues, ou pour lesquels les divers responsables du traitement des données ont une relation complètement différente avec la finalité poursuivie tant sur le plan de la structure ou des ressources que de la capacité de chaque responsable à respecter les règles dans certaines circonstances données, le principe de limitation des finalités est compromis formellement et de façon substantielle et, par conséquent, le principe de proportionnalité ne sera pas non plus dûment appliqué ».

Ainsi, afin de respecter le principe de la limitation des finalités, le projet de loi devrait préciser les finalités pour lesquelles les autorités nationales peuvent recevoir des données.

De plus, la CNPD ne peut que se rallier à l'avis du Conseil d'État relatif à l'article 1er du projet de loi n°7216A concernant les « autorités nationales », selon lequel les auteurs du projet de loi devraient restreindre l'accès aux *« officiers de police judiciaire agréés par le directeur général de la Police grand-ducale ou le directeur de l'Administration des douanes et accises »* et devraient supprimer le point h), à savoir l'Administration des douanes et accises.

Quant à la forme de la demande, à savoir « sur demande », il est encore utile de rappeler que les autorités publiques, telles que les autorités fiscales et douanières, les cellules d'enquête financière, les autorités administratives indépendantes ou les autorités des marchés financiers responsables de la réglementation et de la surveillance des marchés de valeurs mobilières, qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires. 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 et le traitement de données par les autorités publiques en question doit être conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement[50].

Quant aux professionnels, le projet de loi exige que les trustees et les fiduciaires fournissent aux professionnels, sur demande, aux seules fins de la mise en œuvre de leur obligation de vigilance découlant de la loi modifiée du 12 novembre 2004 *« des informations sur les avoirs du trust et le patrimoine des fiducies détenus ou gérés dans le cadre de la relation d'affaires »* (l'article 6, paragraphe 2 du projet de loi). Selon le commentaire des articles, cette disposition assure la mise en œuvre des exigences découlant

[50] Article 4, point 9 et considérant 31 du RGPD, article 2, paragraphe 1er, point 10 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, article 3, point 10 et considérant 22 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.

de la note interprétative de la recommandation 25, point 2 du GAFI[51]. Faute d'explications dans le projet de loi, la CNPD n'est pas en mesure d'apprécier la nécessité et la proportionnalité d'une telle disposition.

III. Quant à l'article 8, paragraphes 5 et 6

En sus de l'obligation prévue à l'article 5 du projet de loi, l'article 8, paragraphes 5 et 6 du projet de loi oblige les fiduciaires et les trustees, respectivement, les professionnels à fournir, sur demande, toute information qu'ils détiennent sur toute fiducie ou tout trust aux personnes visées à l'article 1er, paragraphe 1er, point 1er, lettres a) à c) et point 2 du projet de loi, à savoir le procureur général d'État, les procureurs d'État ainsi que les membres de leurs parquets, les juges d'instruction, la CRF et les autorités de contrôle. Etant donné que l'article 5 du projet de loi oblige les trustees et les fiduciaires à transmettre les informations relatives à toute fiducie et tout trust exprès, la disposition sous revue semble concerner tout trust et non seulement les trusts exprès.

A part la mention que les dispositions assurent la mise en œuvre des exigences découlant de la note interprétative 25, point 4 du GAFI, le commentaire des articles ne fournit aucune explication sur la nécessité ou la proportionnalité d'une telle obligation additionnelle[52]. Il ressort de l'article 31, paragraphe 3 de la directive 2015/849 que les autorités compétentes et les CRF doivent pouvoir accéder en temps utile aux informations visées aux paragraphe 1 de l'article 31, à savoir aux informations collectées par *« les fiduciaires/trustees de toute fiducie expresse/de tout trust exprès »*. Par ailleurs, les dispositions ne mentionnent pas les finalités pour lesquelles les personnes indiquées à l'article 1er, paragraphe 1er, point 1er, lettres a) à c) et point 2 du projet de loi pourraient recevoir les données. S'y ajoute que toute information sur toute fiducie ou tout trust pourrait être demandée. S'agit-il des données visées à l'article 14 du projet de loi ou encore d'autres données ? Par ailleurs, les responsables de traitement qui doivent transmettre les informations aux personnes indiquées à l'article 1er, paragraphe 1er, point 1er, lettres a) à c) et point 2 du projet de loi ne sont pas définis avec précision, de sorte que le champ d'application de cette disposition est incertain et vague.

IV. Quant au registre (chapitres 3 à 5)

a. Quant aux rôles et responsabilités (articles 16 à 18)

La CNPD note que l'AED serait à considérer comme le responsable du traitement au sens du RGPD (article 16, paragraphe 1er du projet de loi) pour le registre des fiducies et des trusts, dont les finalités sont la conservation et la mise à disposition des informations visées à l'article 14 (article 12 du projet de loi). Le Centre des technologies et de l'information de l'État serait à considérer comme le sous-traitant au sens du RGPD (article 16, paragraphe 5 du projet de loi).

[51] Projet de loi n°7216B, doc. parl n°7216B/03, Commentaire des articles, p. 12.
[52] Projet de loi n°7216B, doc. parl n°7216B/03, Commentaire des articles, p. 12.

Le projet de loi précise que l'AED n'est pas responsable du contenu de l'information inscrite (article 16, paragraphe 3 du projet de loi), mais qu'elle peut refuser une inscription incomplète ou non conforme aux dispositions légales ou réglementaires (article 18 du projet de loi).

La CNPD se demande sur base de quels documents ou données l'AED vérifierait la conformité de l'inscription. Aucune précision n'est fournie ni dans le projet de loi, ni dans le commentaire des articles.

Pour le cas où il est envisagé que l'AED consulte des bases de données de tiers pour vérifier l'exactitude des données, de telles consultations devraient être prévues par la loi, qui précise les bases de données à consulter, les modalités de la consultation et les mesures de sécurité.

Quant à l'article 18, paragraphe 2 du projet de loi, celui-ci prévoit qu'en cas de refus d'une demande d'inscription, le requérant doit introduire les pièces justificatives requises, sans pour autant indiquer les pièces justificatives qui pourraient être demandées.

La Commission nationale s'interroge sur la nécessité et la proportionnalité de la transmission des pièces justificatives à l'AED et de la conservation de ces pièces par ce dernier. La directive 2015/849 ne fait aucune mention des pièces justificatives dans le cadre des informations contenues dans le registre. Par ailleurs, comme soulevé ci-avant, l'article 2 du projet de loi oblige les fiduciaires et les trustees à obtenir et à conserver des informations relatives aux bénéficiaires effectifs et l'article 5 les oblige à transmettre ces informations aux autorités nationales et aux organismes d'autorégulation, sur demande.

La CNPD est dès lors à se demander s'il est nécessaire que des pièces justificatives soient transmises à l'AED et conservées par cette dernière. Nonobstant ceci, dans le mesure où le trust ou la fiducie devrait transmettre des pièces justificatives à l'AED, il convient d'indiquer la nature ou les catégories de ces pièces dans un texte légal. En défaut d'une telle indication, les responsables du traitement risqueraient de transmettre des informations non-pertinentes.

b. <u>Quant à l'accès au registre par les autorités nationales, les organismes d'autorégulation et les professionnels (articles 25 et 26)</u>

Quant aux finalités de l'accès au registre, il ressort de l'article 25 du projet de loi sous avis que les autorités nationales ont accès aux informations visées à l'article 14 du projet de loi « dans l'exercice de leurs missions » sans que ces missions soient précisées. L'article 26 précise que les organismes d'autorégulation pourront accéder aux données *« dans l'exercice de leur mission de surveillance en matière de lutte contre le blanchiment et contre le financement du terrorisme »*.

A l'instar de ses remarques faites au point III, la CNPD estime nécessaire de préciser les missions des autorités nationales aux fins desquelles elles peuvent accéder aux données détenues dans le registre, afin de circonscrire clairement l'accès à ces données et l'utilisation qui peut en être faite.

Quant aux données accessibles, le projet de loi utilise la même formulation pour encadrer l'accès au registre par les autorités nationales, les organismes d'autorégulation et les professionnels. Ainsi, ceux-ci *« ont accès aux informations visées à l'article 14 inscrites dans le Registre des fiducies et des trusts »*[53]. Ces mêmes données seront, à l'avenir, également disponibles par l'intermédiaire du système d'interconnexion des registres nationaux, conformément à la législation nationale de l'État membre mettant en œuvre les dispositions de la directive 2015/849 (article 31, paragraphe 9 de la directive 2015/849). L'article 33, paragraphe 2 du projet de loi, qui transpose ladite disposition de la directive, indique ainsi que les données visées en son article 14 seront disponibles *« conformément aux modalités d'accès prévues par la présente loi et les mesures prises pour son exécution »*.

La CNPD se demande si la formulation des articles 25, paragraphe 1er et 26, paragraphe 1er et 2 implique que les modalités d'accès au registre, y compris les données accessibles et les critères de recherche, seront identiques pour les autorités nationales, les organismes d'autorégulation et les professionnels. Par ailleurs, est-ce qu'il est visé de permettre aux autorités nationales, aux organismes d'autorégulation et aux professionnels d'accéder aux données conservées dans le registre conformément à l'article 20 du projet de loi ? Or, dans le cadre de la loi du 13 janvier 2019, les organismes d'autorégulation et les professionnels ne peuvent accéder qu'à une sélection limitée des données enregistrées dans le registre des bénéficiaires effectifs au moment de la consultation, à savoir le nom, le(s) prénom(s), la (ou les) nationalité(s), le jour de naissance, le mois de naissance, l'année de naissance, le lieu de naissance, le pays de résidence, la nature des intérêts effectifs détenus et l'étendue des intérêts effectifs détenus (article 12 de la loi du 13 janvier 2019). Par ailleurs, les critères de recherche ne sont pas identiques pour les professionnels et les organismes d'autorégulation, d'une part, et les autorités nationales, d'autre part. Etant donné que tout traitement de données doit être limité à ce qui est strictement nécessaire et en tenant également en compte l'article 31, paragraphe 9, alinéa 3 de la directive 2015/849, qui exige explicitement que l'accès par l'intermédiaire du système d'interconnexion des registres aux informations renseignées dans le registre doit se faire *« dans le respect des règles en matière de protection des données »*, il se pose entres autres la question de la nécessité pour les professionnels d'avoir accès à toutes les données renseignées dans le registre dans le cadre du projet de loi sous avis. Au vu de ce qui précède, la CNPD considère que la formulation actuelle du projet de loi permet un accès trop large au registre et estime nécessaire de préciser dans le texte du projet de loi les modalités d'accès au registre, y compris les données accessibles et les critères de recherche, dans le respect des règles en matière de protection des données, en particulier en limitant l'accès aux seules données nécessaires. En ce qui concerne les professionnels, il s'agit tout au plus des données considérées comme étant nécessaires dans le cadre de la loi du 13 janvier 2019.

[53] Article 25, paragraphe 1er du projet de loi en ce qui concerne les autorités nationales, l'article 26, paragraphe 1er du projet de loi en ce qui concerne les organismes d'autorégulation et l'article 26, paragraphe 2 du projet de loi en ce qui concerne les professionnels.

La Commission nationale note finalement que les modalités d'accès pour les autorités nationales seront fixées par règlement grand-ducal. Elle regrette que le projet de règlement grand-ducal n'accompagne pas le projet de loi, ce qui lui aurait permis d'analyser l'ensemble du futur cadre légal.

c. <u>Quant à l'accès par le grand public sur base de l'intérêt légitime (article 27)</u>

L'article 27 du projet de loi accorde un accès à certaines données renseignées dans le registre *« sur base d'une décision au cas par cas du directeur de l'AED ou de son délégué, à toute personne physique ou morale qui démontre un intérêt légitime dans le cadre de la prévention de l'utilisation du système financier aux fins de blanchiment ou de financement du terrorisme »*. Cette disposition vise à transposer l'article 31, paragraphe 4 de la directive 2015/849. Il convient à cet égard de rappeler le considérant 28 de la directive 2018/843 qui précise que *« Quand ils fixent le niveau de transparence des informations sur les bénéficiaires effectifs de ces fiducies/trusts ou constructions juridiques similaires, les États membres devraient dûment tenir compte de la protection des droits fondamentaux des personnes, notamment du droit à la vie privée et du droit à la protection des données à caractère personnel. »*.

La collecte et la mise à disposition des données des personnes concernées, à savoir les bénéficiaires effectifs des trusts et fiducies, constitue une ingérence dans les droits fondamentaux au respect de la vie privée et familiale et à la protection des données à caractère personnel consacrés par les articles 7 et 8 de la Charte des droits fondamentaux (ci-après « la Charte »). Conformément à l'article 52, paragraphe 1er de la Charte, l'exercice de ces droits peut être limité, à condition que :

- l'ingérence soit prévue par la loi ;
- l'ingérence respecte le contenu essentiel des droits et libertés ;
- l'ingérence est nécessaire, sous réserve du principe de proportionnalité ; et
- l'ingérence répond effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

Afin d'être proportionnel, le législateur doit s'assurer que les actes sont *« aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs »*[54].

En ce qui concerne la balance entre la transparence et la protection des données à caractère personnel, la Cour de Justice a jugé que *« les institutions sont tenues de mettre en balance, avant de divulguer des informations concernant une personne physique, l'intérêt de l'Union à garantir la transparence de ses actions et l'atteinte aux droits reconnus par les articles 7 et 8 de la Charte. Aucune prééminence automatique ne saurait être reconnue à l'objectif de transparence sur le droit à la protection des données à caractère personnel […], même si des intérêts économiques importants sont en jeu. »*[55].

[54] Arrêt du 8 avril 2014, Digital Rights Ireland, C-293/12 et C-594/12, EU:C:2014:238, point 46 et les jurisprudences y citées.
[55] Arrêt du 9 novembre 2010, Volker und Markus Schecke, C-92/09 et C-93/09, EU:C:2010:662, point 85.

En conséquence, le législateur devrait être en mesure de démontrer que les dérogations et les limitations se limitent au stricte nécessaire.

i. Les données accessibles

Ces personnes pourraient accéder au nom, aux prénoms, aux nationalités, au mois et à l'année de naissance, au pays de résidence ainsi qu'à la nature de l'implication de la personne concernée dans la fiducie ou dans le trust et l'étendue des intérêts effectifs détenus (article 27, paragraphe 1er du projet de loi). La CNPD salue le choix des auteurs du projet de loi de limiter l'accès aux seules données requises par l'article 31, paragraphe 4, alinéa 2 de la directive 2015/849.

ii. La condition de l'intérêt légitime

Quant à la condition de l'intérêt légitime, le projet de loi précise dans son article 27, paragraphe 2, alinéa 4 que le demandeur doit joindre *« tout document de nature à justifier l'existence d'un intérêt légitime »*. Par ailleurs, le paragraphe 3 énonce qu'*« aux fins de l'appréciation de l'existence d'un intérêt légitime, le directeur de l'AED ou son délégué tient compte de toute circonstance pertinente, susceptible d'indiquer si l'accès à l'information est demandé en vue d'une contribution à la détection ou à la poursuite de violations de la législation relative à la lutte contre le blanchiment et contre le financement du terrorisme »*.

En outre, le directeur de l'AED ou son délégué tient compte de la protection des droits fondamentaux des personnes, notamment du droit à la vie privée et du droit à la protection des données à caractère personnel lors de sa prise de décision ».

Il ressort du commentaire des articles que le directeur de l'AED ou son délégué peut fonder sa décision sur tous les faits relatifs à la demande qui lui est soumise, y compris ceux qui n'auraient pas été soulevés par la personne physique ou morale demanderesse[56].

Selon le considérant 28 de la directive 2018/843, *« les critères et les conditions d'octroi de l'accès aux demandes d'informations sur les bénéficiaires effectifs des fiducies/trusts et des constructions juridiques similaires devraient être suffisamment précis et conformes aux objectifs de la présente directive »*. Ainsi, *« les États membres devraient définir l'intérêt légitime dans leur droit national, à la fois en tant que notion générale et en tant que critère déterminant l'accès aux informations sur les bénéficiaires effectifs »* (considérant 42 de la directive 2018/843).

Ainsi, afin de satisfaire à l'exigence de prévisibilité, la loi devrait comporter des critères objectifs permettant de définir la notion d'« intérêt légitime » de manière précise et non équivoque[57] et les critères sur lesquelles se fonderait la décision par le directeur de l'AED ou de son délégué. La simple mention dans le commentaire des articles que

[56] Projet de loi n°7216B, doc. parl n°7216B/03, Commentaire des articles, p. 23.
[57] Avis du 16 décembre 2016 du service juridique du Conseil de l'Union européenne, doc 15655/16, point 47.

la décision pourrait être fondée sur tous les éléments relatifs à la demande n'est pas suffisamment claire pour satisfaire à l'exigence de prévisibilité et de précision d'une loi.

Une définition claire de l'intérêt légitime est importante, car, comme l'a soulevé à juste titre le CEPD, une définition trop large du concept d'intérêt légitime risquerait d'encourager les personnes souhaitant accéder à ces informations pour des raisons purement opportunistes[58]. Il convient dès lors d'exiger un lien direct entre la justification et l'intérêt et exiger que l'utilisation des informations obtenues contribue manifestement à la réalisation de l'objectif public en question[59].

Ainsi, comme l'a précisé le service juridique du Conseil de l'Union européenne lors de l'élaboration de la directive 2018/843, *« il serait nécessaire d'intégrer au dispositif de la proposition une définition contenant des critères objectifs et vérifiables. En d'autres termes, les déclarations de mission auto-proclamées d'organisations axées sur la transparence (ou, accessoirement, sur la lutte contre le blanchiment de capitaux) ne sauraient être considérées comme suffisantes en soi, mais elles doivent être combinées à une preuve attestant que l'utilité publique des actions menées par l'organisation dans ce domaine a été reconnue de manière indépendante. »*[60].

La définition d'« intérêt légitime » devrait prévoir au moins qu'une personne ne pourrait accéder aux données que si *« elle est en mesure de démontrer aux autorités nationales compétentes qu'elle a la capacité et l'intention d'utiliser ces informations pour le seul intérêt public en cause (qui doit être défini avec précision), et ce d'une manière ne portant pas atteinte de façon disproportionnée au droit au respect de la vie privée, et si elle accepte d'être soumise à l'autorisation et au contrôle des autorités nationales compétentes dans l'exercice de toute activité où il est fait usage de l'ensemble ou d'une partie des informations ainsi obtenues »*[61].

iii. <u>Les données nécessaires pour obtenir accès au registre</u>

Il ressort de l'article 27, paragraphe 2 du projet de loi qu'une personne physique souhaitant obtenir des informations du registre sur base de son intérêt légitime doit fournir les données à caractère personnel suivantes à l'appui de sa demande: ses noms, prénoms, nationalités, date de naissance, lieu de naissance et domicile ou résidence. La personne demanderesse doit encore fournir un extrait du casier judiciaire.

Aucune information n'est fournie quant à la nécessité de ces données et du casier judiciaire, le commentaire des articles se limitant à expliquer que *« le casier judiciaire devra être donné pour chaque personne qui aura accès aux données divulguées »*[62].

Par ailleurs, le projet de loi ne précise ni quel type de bulletin du casier judiciaire devrait être fourni, ni la durée de rétention du casier judiciaire suite au dépôt de la demande d'accès au registre. La CNPD s'interroge encore sur l'imprécision de la formulation employée dans le corps du projet de loi par rapport à la précision dans le commentaire des articles sur les personnes devant fournir un casier judiciaire. En effet, si plusieurs personnes

[58] Avis 1/2017 du Contrôleur européen sur la proposition de la Commission modifiant la directive (UE) 2015/849 et la directive 2009/101/CE, point 59.
[59] Avis du 16 décembre 2016 du service juridique du Conseil de l'Union européenne, doc 15655/16, point 46.
[60] Avis du 16 décembre 2016 du service juridique du Conseil de l'Union européenne, doc 15655/16, point 49.
[61] Avis du 16 décembre 2016 du service juridique du Conseil de l'Union européenne, doc 15655/16, point 49.
[62] Projet de loi n°7216B, doc. parl. n°7216B/03, page 22.

auraient accès aux données, il s'ensuit que les casiers judiciaires de toutes ces personnes devraient être fournis. Qu'en-est-il de la demande faite par une personne morale, faut-il également fournir un casier judiciaire de toutes les personnes engagées auprès de la personne morale qui pourraient avoir accès aux données? S'il tel est le cas, est-ce que l'employeur devrait les collecter et les transmettre à l'AED ou est-ce que les employés seraient censés les transmettre individuellement?

En l'absence d'une explication de la nécessité et de la proportionnalité de ces données et de plus de précision dans le corps du texte, la CNPD n'est pas en mesure d'analyser la conformité de la disposition à la législation en matière de protection des données.

iv. L'utilisation des données obtenues

Par ailleurs, selon le paragraphe 4, l'extrait comportant les informations sur les bénéficiaires effectifs fourni en cas de décision favorable *« indique l'utilisation aux fins de laquelle l'accès est accordé. La personne physique ou morale demanderesse ne peut utiliser l'information à des fins autres que celles précisées par l'extrait »*. La CNPD estime que l'utilisation aux fins de laquelle l'accès est accordé devrait se situer exclusivement dans le contexte du projet de loi et ne peut en aucun cas aller au-delà de ce cadre. Elle s'interroge ainsi sur le pouvoir du directeur de l'AED ou de son délégué de déterminer les finalités aux fins desquelles peuvent servir les données provenant du registre et elle considère que la disposition devrait être précisée afin de circonscrire ce pouvoir.

d. Quant à l'accès aux informations relatives à une fiducie ou un trust qui détient ou possède une participation de contrôle dans une société ou dans une autre entité juridique autres que celles visées à l'article 30 de la directive 2015/849 (article 29)

L'article 29 du projet de loi transpose l'article 31, paragraphe 4, lettre d) de la directive 2015/849, en accordant un accès aux informations relatives à une fiducie ou un trust qui détient ou possède une participation de contrôle dans une société ou dans une autre entité juridique autres que celles visées à l'article 30, paragraphe 1er de la directive (UE) 2015/849 par propriété directe ou indirecte, notamment au moyen d'actions au porteur ou par le biais d'un contrôle par d'autres moyens, à toute personne physique ou morale qui introduit une demande écrite portant sur une telle fiducie ou un tel trust. Selon le considérant 28 de la directive 2018/843, *« Les États membres devraient pouvoir refuser une demande écrite s'il existe des motifs raisonnables de soupçonner que la demande écrite n'est pas conforme aux objectifs de la présente directive. »*. La CNPD note que les auteurs du projet de loi n'ont pas repris cette possibilité dans la loi en projet.

Par ailleurs, le projet de loi n'encadre pas cet accès. Par exemple, il ne détermine ni quelles informations devant accompagner la demande d'accès, ni comment identifier le trust ou la fiducie, ni le délai endéans lequel l'AED doit répondre à la demande. Le projet de loi devrait dès lors être amendé afin d'encadrer clairement cet accès.

e. Quant à l'interconnexion du registre (article 33)

L'article 33 du projet de loi encadre la future interconnexion du registre avec les registres instaurés dans les autres États membres. Les informations visées à l'article 14 inscrites dans le Registre des fiducies et des trusts sont disponibles par l'intermédiaire du système d'interconnexion des registres institué par l'article 22, paragraphe 2, de la directive (UE) 2017/1132 conformément aux modalités d'accès prévues par le projet de loi et les mesures prises pour son exécution (paragraphe 2).

La directive 2015/849 dispose que seules les informations qui sont à jour et qui correspondent aux véritables bénéficiaires effectifs doivent être mises à disposition par l'intermédiaire du registre national et du système d'interconnexion des registres. L'accès à ces informations doit avoir lieu dans le respect des règles en matière de protection des données (article 31, paragraphe 9, alinéa 3 de la directive 2015/849). Dès lors, au cas où des données incorrectes auraient été mises à disposition, il convient d'assurer que l'AED transmette les données corrigées ultérieurement aux destinataires conformément à l'article 19 du RGPD.

A l'instar de l'avis du CEPD sur la proposition de directive du Parlement européen et du Conseil modifiant les directives 89/666/CEE, 2005/56/CE et 2009/101/CE en ce qui concerne l'interconnexion des registres centraux, du commerce et des sociétés, la CNPD relève qu'une meilleure accessibilité des données à caractère personnel entraîne également des risques accrus pour celles-ci[63].

Quant aux données accessibles et les finalités de l'accès, étant donné que les données enregistrées seront disponibles par l'intermédiaire du système d'interconnexion des registres, la CNPD se demande si toutes les données prévues à l'article 14, y compris le numéro d'identification national (« matricule ») au sens de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, devraient être accessibles. Elle se réfère à cet égard aux remarques faites ci-avant au point II. Par ailleurs, il convient d'assurer le respect du principe des finalités, même lors des échanges de données.

Quant à la durée de conservation des données, l'article 33, paragraphe 3 de la loi en projet prévoit que les données visées à l'article 14 sont disponibles par l'intermédiaire du système d'interconnexion des registres pendant cinq ans après que les motifs de l'inscription visés à l'article 13, paragraphes 1er ou 2 ont cessé. La directive laissant aux États membres le choix entre une durée minimale de cinq ans et une durée maximale de dix ans, la CNPD se félicite du choix des auteurs du projet de loi de limiter l'accès aux données à cinq ans.

V. Quant aux droits des personnes concernées

Pour ce qui est du responsable du traitement du registre des bénéficiaires effectifs, à savoir l'AED, celui-ci collectera les données de manière indirecte et devra, dès lors, en principe fournir toutes les informations prévues à l'article 14

[63] Avis du 6 mai 2011 Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil modifiant les directives 89/666/CEE, 2005/56/CE et 2009/101/CE en ce qui concerne l'interconnexion des registres centraux, du commerce et des sociétés, (2011/C 220/01), point 21.

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 »*. A cet égard, 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 UBO, que le responsable du traitement devrait informer chaque personne physique de son inscription dans le registre[64]. 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. La Commission nationale estime que cette information devrait avoir lieu endéans les délais prévus à l'article 14, paragraphe 3 du RGPD.

Il convient encore de souligner que les trustees et les fiduciaires, 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. Afin de protéger les personnes concernées, le responsable du traitement devrait informer les personnes concernées des spécificités de l'enregistrement de leurs données. Les auteurs du projet de loi pourraient s'inspirer de l'article 21 de l'arrêté royal belge du 30 juillet 2018 relatif aux modalités de fonctionnement du registre UBO.

Pour ce qui est du droit à la rectification, la CNPD note que le projet de loi prévoit un régime spécifique quand des personnes constatent une divergence entre les informations sur les bénéficiaires effectifs disponibles dans le registre et les informations sur les bénéficiaires effectifs dont elle dispose et en informent l'AED (article 19 du projet de loi). Pour informer les personnes consultant le registre que les données ont été déclarées comme étant incorrectes, une mention est insérée dans le registre et les personnes demandant accès sont informées qu'une mise à jour a été demandée (article 19, alinéa 3 du projet de loi). Dans un souci de clarté, il pourrait être opportun d'ajouter au projet de loi une disposition précisant la procédure de rectification des données à suivre par la personne concernée, à l'instar de la procédure décrite à l'article 23 de l'arrêté royal belge du 30 juillet 2018 relatif aux modalités de fonctionnement du registre UBO :

« § 1er. Toute personne physique peut, directement ou par l'intermédiaire de l'Administration de la Trésorerie, demander sans frais au redevable d'information dont il est le bénéficiaire effectif la rectification ou la suppression des données inexactes enregistrées à son nom.

[64] *« Les redevables d'information informent leurs bénéficiaires effectifs sur un support durable: 1° de l'obligation dans le chef des redevables d'information de communiquer au registre les données visées aux articles 3 et 4 ; 2° de l'enregistrement et de la conservation de ces données dans le registre ; 3° du nom et de l'adresse du service chargé de la gestion du registre au sein de l'Administration de la Trésorerie ; 4° de l'accès possible au registre des entités et personnes listées aux articles 6 et 7 ; 5° du droit du bénéficiaire effectif, conformément à l'article 22, de prendre connaissance des données enregistrées à son nom dans le registre ; 6° du droit du bénéficiaire effectif à la rectification et à la suppression des données inexactes enregistrées à son nom dans le registre, qui doit être exercé auprès du redevable d'information concerné conformément à l'article 23 ; 7° du délai de conservation des données enregistrées dans le registre déterminé à l'article 25.*
L'Administration de la Trésorerie informe les bénéficiaires effectifs de leur inscription dans le registre et leur communique les informations enregistrées à leur nom. »

§ 2. Le redevable d'information est tenu, sous sa responsabilité exclusive, de rectifier ou supprimer les données inexactes enregistrées en rapport avec ses bénéficiaires effectifs dans ses propres fichiers et de communiquer sans délai ces modifications au registre. »

VI. Quant à la coopération entre la CRF, les autorités de contrôle et les organismes d'autorégulation (article 32)

Il ressort de l'article 32 du projet de loi que la CRF, les autorités de contrôle et les organismes d'autorégulation coopèrent étroitement entre eux. Quant à la forme et les finalités de la coopération, l'alinéa 2 précise que *« 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. »*

Aucune information n'est fournie ni sur la forme, ni sur les finalités de la coopération entre la CRF, les autorités de contrôle et les organismes d'autorégulation. Plus précisément, le projet de loi n'indique pas si les organismes d'autorégulation pourraient échanger des données avec la CRF et les autorités de contrôle.

Si malgré ceci les organismes d'autorégulation pourraient être amenés à échanger des données à caractère personnel avec la CRF et les autorités de contrôle, le Conseil d'État a souligné à plusieurs reprises que la communication de données informations à des tiers peut constituer une ingérence dans la vie privée[65] et constitue ainsi en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Il faut donc que les points essentiels soient fixés par la loi.

Ainsi, dans la mesure où la CRF, les autorités de contrôle et les organismes d'autorégulation échangeraient des données à caractère personnel, le projet de loi devrait encadrer la coopération de ces responsables du traitement, en précisant la forme et la finalité de cette coopération pour tous les responsables du traitement, y compris les organismes d'autorégulation.

Quant à la coopération internationale, l'article 32, paragraphe 2 du projet de loi instaure un cadre légal de coopération internationale par lequel les autorités de contrôle coopèrent avec leurs autorités homologues étrangères dans le respect des limites des dispositions de l'article 9-2 de la loi modifiée du 12 novembre 2004. Or, il ressort de l'article 31, paragraphe 7 de la directive 2015/849 que *« les États membres veillent à ce que les autorités compétentes et les CRF soient en mesure de fournir, en temps utile et gratuitement, les informations visées aux paragraphes 1 et 3 aux autorités compétentes et aux CRF d'autres États membres »*. La directive envisage dès lors un échange européen et non pas un échange avec des pays tiers. En l'absence d'une analyse de la nécessité et la proportionnalité de l'extension de ce régime de coopération aux pays tiers, la CNPD estime que ces dispositions devraient se limiter à transposer les dispositions de la directive 2015/849.

[65] Avis du Conseil d'État du 21 novembre 2017 relatif au projet de loi n°7182, doc. parl. 7182/02, page 7.

ANNEXES

5

Ainsi décidé à Esch-sur-Alzette en date du 28 février 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

Avis complémentaire relatif au projet de loi n°7216B portant transposition de l'article 31 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, tel que modifié 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/UE.

(Délibération n°9/2020 du 3 avril 2020)

1. 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 »*.

2. En date du 28 février 2020, la CNPD a avisé le projet de loi n°7216B portant transposition de l'article 31 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, tel que modifié 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/UE (ci-après « le projet de loi »).

3. En date du 31 mars 2020, Monsieur le Ministre des Finances, a invité la Commission nationale à se prononcer au sujet des amendements parlementaires au projet de loi, adoptés le 30 mars 2020 par la Commission des Finances et du Budget de la Chambre des Députés.

Quant à l'article 3 du projet de loi

4. L'amendement 2 concerne l'article 3 du projet de loi et plus précisément l'obligation pour les trustees et les fiduciaires d'obtenir et de conserver des informations élémentaires sur les autres agents réglementés et prestataires de services du trust ou de la fiducie. La CNPD, dans son avis du 28 février 2020, et le Conseil d'État, dans son avis du 24 mars 2020, ont estimé que cette disposition n'était pas formulée de manière suffisamment précise.

5. Suite à l'amendement 2, l'article précise dorénavant que cette obligation concerne tous les autres professionnels visés à l'article 2 de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme qui prestent des services au trust ou à la fiducie ou qui entrent en relation d'affaires avec le trust ou la fiducie. Le nouvel alinéa 2 précise quelles informations doivent être obtenues et conservées par les trustees et les fiduciaires, à savoir les informations qui permettent *« aux trustees et aux fiduciaires d'identifier les personnes concernées et comprennent dans le cas d'une personne physique les informations visées à l'article 14, paragraphe 2 point 1, lettres a) à c) et h) à i) »*. Plus précisément, il s'agit des nom et prénom, de la nationalité, du pays de résidence et de l'adresse privée ou professionnelle de la personne physique.

6. La Commission nationale s'interroge encore sur la nécessité et la proportionnalité de collecter ces données de « tous les autres professionnels qui prestent des services au trust ou à la fiducie ou qui entrent en relation d'affaires avec le trust ou la fiducie ». En tenant compte de ses remarques faites au point 7 ci-après et comme une telle obligation pourrait conduire à la collecte d'une multitude de données de beaucoup de personnes concernées, elle réitère ses remarques faites dans son avis du 28 février 2020 relatives à l'analyse de la nécessité et de la proportionnalité d'une telle obligation.

7. Alors que la CNPD accueille favorablement la précision à l'alinéa 2 à l'article 3, paragraphe 1er du projet de loi, elle regrette que la disposition ne délimite pas clairement les données à collecter, mais prévoie plutôt que les données à collecter « comprennent » les informations visées à l'article 14, paragraphe 2 point 1, lettres a) à c) et h) à i). Dans un objectif de minimisation de données, elle suggère de supprimer les mots *« et comprennent »* de la disposition.

Quant à l'article 27 du projet de loi

8. La CNPD prend note du complément d'explications relatif à l'article 27, paragraphe 2, alinéa 3 du projet de loi, à savoir la condition de devoir fournir un extrait du casier judiciaire en vue de se voir accorder, sur base d'un l'intérêt légitime, l'accès à certaines données contenues dans le Registre des fiducies et des trusts. Selon ces explications, le casier judiciaire serait nécessaire pour vérifier si un demandeur justifie de garanties suffisantes

d'honorabilité. Si le Conseil d'État n'estime pas que les explications seraient suffisantes pour justifier le respect des principes de nécessité et d'adéquation, la Commission des Finances et du Budget propose de supprimer l'obligation de fournir un extrait de casier judiciaire.

9. La CNPD se félicite des précisions relatives aux droits fondamentaux des personnes concernées inscrites au Registre des fiducies et des trusts ainsi que des explications quant à la nécessité de fournir un extrait du casier judiciaire. Elle comprend que cette exigence vise à protéger les personnes concernées inscrites au registre. Elle constate cependant avec regret que ces explications ne répondent pas aux questions soulevées par la CNPD dans son avis du 28 février 2020 et à celles soulevées par le Conseil d'État dans son avis du 24 mars 2020. Par ailleurs, tout comme le Conseil d'État, la CNPD s'interroge sur le lien entre l'extrait du casier judiciaire et l'accès au registre. Est-ce que l'accès serait systématiquement refusé aux personnes ne disposant pas d'un extrait de casier judiciaire vierge ?

10. Par ailleurs, la Commission nationale s'interroge sur les deux options présentées par les auteurs : (a) maintenir l'exigence de fournir un extrait du casier judiciaire, sans prévoir des garanties visant à encadrer le traitement de l'extrait de casier judiciaire, ou (b) supprimer cette obligation du projet de loi sans la remplacer par d'autres mesures visant à protéger les personnes concernées inscrites au registre contre d'éventuels abus. En effet, ces options ne répondent pas vraiment aux questions soulevées par la CNPD et le Conseil d'État. Au cas où les auteurs souhaiteraient supprimer l'obligation de fournir un extrait du casier judiciaire, la CNPD note encore que le projet de loi n'exige pas qu'un demandeur doive fournir une pièce d'identité à l'appui de sa demande et s'interroge sur l'absence d'une telle obligation. En tout état de cause, comme les auteurs souhaitent, à juste titre, protéger les droits fondamentaux des personnes concernées inscrites, les auteurs pourraient prévoir d'autres mesures, telles que p.ex. une preuve des mesures de sécurité qui seraient mises en œuvre par le demandeur pour protéger les données ou encore l'exigence davantage de documents démontrant l'intérêt légitime (par exemple, des informations qui démontrent des suspicions qu'un trust ou une fiducie est utilisé ou a été utilisé aux fins de blanchiment ou de financement du terrorisme).

11. Finalement, la CNPD regrette que les auteurs du projet de loi n'aient pas suivi ses autres recommandations formulées dans son avis du 28 février 2020.

Ainsi décidé à Esch-sur-Alzette en date du 3 avril 2020.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann	Marc Lemmer
Présidente	Commissaire	Commissaire	Commissaire

ANNEXES

5

Avis complémentaire relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

(Délibération n°10/2020 du 17 avril 2020)

Conformément à l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n°2016/680 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 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 »), à laquelle se réfère l'article 8 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 (ci-après 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 la « Commission nationale » ou la « CNPD »), « conseille la Chambre des députés, 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 des données personnelles ».

En date du 28 février 2020, la CNPD a avisé le projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale (ci-après le « projet de loi »).

En date du 6 avril 2020, Monsieur le Ministre de la Sécurité intérieure a invité la Commission nationale à se prononcer au sujet de l'amendement gouvernemental au projet de loi qui a été approuvé par le Conseil de gouvernement dans sa séance du 20 mars 2020 (ci-après l' « amendement gouvernemental »).

Le présent avis complémentaire se limitera à commenter les points 1° et 2° de l'amendement gouvernemental, le point 3° étant accueilli favorablement par la Commission nationale.

1. L'introduction d'un nouveau point 4° au paragraphe 2 de l'article 43bis du projet de loi

Le paragraphe 2 de l'article 43*bis* définit et énumère des critères des lieux présentant un risque particulier de commission de crimes ou délits ou d'atteintes à la sécurité des personnes ou des biens, sans toutefois viser nommément des lieux spécifiques.

Or, l'amendement gouvernemental s'éloigne de cette logique car celui-ci introduit un nouveau point 4° au paragraphe 2 de l'article 43*bis* qui vise spécifiquement un lieu : le stade national de football et de rugby sis à Kockelscheuer.

La Commission nationale se demande dès lors la raison pour laquelle ce lieu spécifique est ajouté alors que les points 1°, 2°, 3° et 5° du paragraphe 2 de l'article 43*bis*, qui ne visent pas de lieu en particulier, demeurent inchangés.

En effet, il ressort de l'économie générale de l'article 43bis paragraphe (2) que l'intention initiale des auteurs du projet de loi était de prévoir une disposition plus générale, susceptible de couvrir tous lieux qui rentrent dans les critères des points 1° à 4°. Dans cette logique il reviendra sur proposition du Directeur de la Police grand-ducale et puis par l'autorisation ministérielle de désigner justement les lieux (zones de sécurité) qui rentrent dans le champ d'application de l'article 43bis.

Une solution alternative aurait été de prévoir dans le projet de loi une liste exhaustive de lieux spécifiques placés sous vidéosurveillance, ce qui, aux yeux de la CNPD, n'aurait pas été recommandable d'un point de vue légistique.

Or, comme pré-mentionné l'amendement sous examen s'écarte de la logique initiale du texte.

La CNPD considère dès lors que l'ajout de ce nouveau point 4° est superfétatoire et suggère de le supprimer, dans la mesure où le stade national de football et de rugby sis à Kockelscheuer est susceptible d'être couvert par les critères prévus pourles lieux visés au point 3°, voire du point 4° du texte initial de l'article 43*bis* du projet de loi.

Cette hypothèse est d'ailleurs expressément visée par les auteurs du projet de loi dans leur commentaire du paragraphe 2 de l'article 43*bis* du projet de loi. En effet, ces derniers y précisent que : *« Le point 3 vise des infrastructures telles que des stades ou centres de conférences où sont organisés régulièrement des évènements d'envergure nationale ou internationale. Comme par le passé, la vidéosurveillance en ces lieux ne sera pas activée en permanence, mais uniquement lors de l'évènement dans le contexte duquel des atteintes aux personnes ou aux biens sont susceptibles de se produire. On peut citer, à titre d'exemples, les alentours du stade Josy BARTHEL à l'occasion d'un match de football international (…) ».*

2. L'utilisation de la notion de « zone de sécurité » à la place du terme « lieu » au paragraphe 3 de l'article 43*bis* du projet de loi

L'amendement gouvernemental a encore pour objet de remplacer le terme « lieu » par la notion de « zone de sécurité » au paragraphe 3 de l'article 43*bis*.

Il ressort du commentaire de l'amendement gouvernemental que les auteurs du projet de loi justifient ce remplacement, afin *« d'assurer la cohérence avec la législation antérieure »* et précisent encore que : *« Le terme*

« zone de sécurité » est également cohérent avec l'article 2 du présent projet de loi qui dispose que le maintien de la vidéosurveillance dans les lieux désignés comme zones de sécurité avant l'entrée en vigueur de la présente loi devra être autorisé conformément aux dispositions de cette dernière dans un délai maximal de douze mois suivant l'entrée en vigueur de la présente loi ».

Il y a d'abord lieu de relever que la notion de « zone de sécurité » introduite au paragraphe 3 de l'article 43*bis* du projet de loi diffère du terme « zone de sécurité » tel qu'utilisé à l'article 2 du projet de loi, dans la mesure où celui-ci fait expressément référence aux lieux désignés comme zones de sécurité sous l'empire de l'ancienne législation. La notion de « zone de sécurité » introduite au paragraphe 3 de l'article 43*bis* doit être comprise dans le contexte du présent projet de loi.

Ainsi et bien que la Commission nationale comprenne la volonté des auteurs du projet de loi de reprendre la notion de « zone de sécurité » afin « d'assurer la cohérence avec la législation antérieure », elle estime nécessaire, pour une meilleure compréhension du paragraphe 3 de l'article 43*bis*, que cette notion soit définie dans le projet de loi.

En effet, l'introduction de la notion de « zone de sécurité », de manière isolée ; à l'endroit du paragraphe 3 de l'article 43*bis*, sans l'avoir préalablement définie, compromet la compréhension dudit paragraphe et ce d'autant plus alors que le terme de « zone de sécurité » est différent de la terminologie utilisée jusqu'à présent par les auteurs du projet de loi dans les paragraphes 2 et 4 de l'article précité.

Si la « zone de sécurité » au sens du paragraphe 3 de l'article 43*bis* désigne un lieu à risque[66] qui a été délimité au préalable par la Police grand-ducale puis communiqué au ministre ayant la Police dans ses attributions afin que celui-ci délivre une autorisation ministérielle pour un tel lieu délimité, alors cela devait ressortir clairement du projet de loi.

Dès lors, si les auteurs de l'amendement gouvernemental souhaitent faire un parallélisme avec l'ancienne législation, il serait nécessaire de définir la notion de « zone de sécurité » ou bien de remplacer le terme « lieux », utilisé à différents endroits à l'article 43bis, par les termes « zone de sécurité », ou bien supprimer les termes « zone de sécurité », afin d'uniformiser en conséquence l'ensemble de la terminologie utilisée dans le projet de loi.

Ainsi décidé à Esch-sur-Alzette en date du 17 avril 2020.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann	Marc Lemmer
Présidente	Commissaire	Commissaire	Commissaire

[66] Au sens du paragraphe 2 de l'article 43bis du projet de loi.

Avis relatif au projet de loi n°7526 portant modification de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

(Délibération n°11/2020 du 24 avril 2020

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 ».*

Par courrier en date du 3 mars 2020, Monsieur le Ministre des Communications a invité la Commission nationale à se prononcer sur le projet de loi n°7526 portant modification de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

Le projet de loi tend à mettre en place un ou des systèmes de géolocalisation des auteurs d'appels de secours plus précis(es) que la géolocalisation actuelle effectuée exclusivement au moyen des bornes du réseau de téléphonie mobile.

Il anticipe la transposition du seul article 109 paragraphe 6 de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

La Commission nationale note que le nouvel article 5 paragraphe (5bis) projeté ne précise pas qui doit mettre à disposition les données en question. On peut en déduire que ce paragraphe crée des obligations exclusivement à charge des fournisseurs de services ou opérateurs mentionnés à l'article 5 paragraphe (5) lettre (a). Si, cependant, d'autres entreprises, comme par exemple les entreprises offrant les systèmes d'exploitations ou des logiciels installés sur les appareils ou des entreprises offrant un accès WIFI sans être des fournisseurs de services ou des opérateurs, étaient tenues de participer – d'une quelconque manière – aux systèmes de géolocalisation en question, il conviendrait de le mentionner dans le texte.

ANNEXES

5

La CNPD s'interroge par ailleurs sur la signification des termes « *… le plus approprié …* » utilisés dans l'article unique du projet de loi et qui sont repris littéralement de l'article 109 paragraphe (6) de la directive (UE) 2018/1972 précité. En effet, en vue d'une transposition correcte de la disposition de la directive européenne en question, elle se demande si, en fonction de la situation ou de l'organisation nationale relatives aux centres de réception d'appels d'urgence, il n'appartient pas au législateur national de désigner ou de définir dans le texte de loi même de quel(s) centre(s) de réception d'appels d'urgence il s'agit précisément.

Ainsi décidé à Esch-sur-Alzette en date du 24 avril 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

Avis relatif au projet de loi n°7606 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre le virus SARS-CoV-2 (COVID-19) et modifiant 1. la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2. la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments.

(Délibération n°13/2020 du 8 juin 2020)

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 ».*

En date du 4 juin 2020, Madame la Ministre de la Santé a saisi la Commission nationale à se prononcer sur le projet n°7606 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre le virus SARS-CoV-2 (COVID-19) et modifiant 1. la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2. la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments (ci-après le « projet de loi »). Dans ledit courrier Madame la Ministre a précisé que le projet en cause devra entrer en vigueur au plus tard le 24 juin 2020, date de la levée de l'état de crise, et que partant, elle nous prie de lui faire parvenir notre avis endéans les plus brefs délais. La CNPD tient à souligner que son avis a ainsi été élaboré et adopté uniquement sur base des informations dont elle dispose et sous réserve d'éventuelles considérations futures non connues à ce jour.

Le présent projet de loi a pour objet de créer un cadre légal se rapportant à des mesures prises à l'égard des personnes physiques pour continuer la lutte contre le Covid-19 en limitant la propagation du SARS-CoV-2 sur le territoire du Grand-Duché de Luxembourg moyennant un catalogue limité de mesures bien circonscrites. Il ressort de l'exposé des motifs qu'à côté des mesures centrées sur les personnes physiques, le projet de loi s'articule autour des trois axes suivants :

- la limitation de la liberté de rassemblement ;

- l'application de mesures de protection ainsi que l'identification, le suivi et la mise à l'écart rapide des personnes infectées et susceptibles d'être infectées ;
- l'instauration de *« certaines garanties autour du traitement des données nécessaires au suivi des personnes et à la lutte contre la pandémie. »*

La Commission nationale tient à souligner à titre préliminaire que la protection des données personnelles n'est pas à considérer comme obstacle à la mise en place d'un traitement de données à caractère personnel dans le cadre de la lutte contre l'épidémie Covid-19, tant que les principes fondamentaux prévus par le RGPD sont respectés. Elle entend ainsi 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, et plus précisément à son article 9.

Ad article 9 du projet de loi n°7606

L'article 9 du projet de loi n°7606 vise la création d'un système d'information par la Direction de la santé, afin de surveiller l'évolution de la situation liée au Covid-19 et de formuler des recommandations dans l'intérêt de la santé publique à l'attention du Gouvernement (ci-après : le « système d'information »). Le commentaire de l'article précise qu'à cette fin, un système de monitoring avec différents indicateurs et types de données est mis en place, incluant tant des données à caractère personnel que des données à caractère non personnel qui doivent obligatoirement être transmises à l'autorité de santé publique.

En vertu du paragraphe (2) de l'article 9 du projet de loi, différentes données à caractère personnel concernant les personnes infectées ou présumées infectées au Covid-19 sont à transmettre à la Direction de la santé par les établissements hospitaliers, les structures d'hébergement et les réseaux de soins en vue de détecter, évaluer, surveiller et combattre le Covid-19. Ces données sont énumérées aux articles 3 et 4 de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique. Étant donné que le projet de loi ne définit pas d'autres catégories de données individuelles à fournir que celles énumérées aux articles 3 et 4 susmentionnées, la Commission nationale estime que le présent article est à lire restrictivement et que nonobstant le fait que l'énumération des données à collecter comprend la précision « au moins », elle ne doit pas être élargie en l'espèce, sinon il faudrait le préciser. La Commission nationale comprend donc qu'il s'agit plus spécifiquement du nom, prénom, adresse, date de naissance, diagnostic médical, date des premiers symptômes et date du diagnostic médical, date de prélèvement et origine du prélèvement, pays où la maladie a été contractée et la source d'infection si connue.

Il est donc indéniable que des catégories particulières de données à caractère personnel, dites données « sensibles », seront traitées à travers ce système d'information. Ces données, incluant les données concernant la santé, sont spécifiquement réglementées par l'article 9 du RGPD. Par principe, il est interdit de traiter des données sensibles, sauf si une des dix conditions prévues au paragraphe (2) de l'article 9 du RGPD est remplie. Sous

réserve des commentaires qui suivent et face à la déclaration du 30 janvier 2020 de l'Organisation mondiale de la santé (OMS) que l'apparition du coronavirus SARS-CoV-2 (Covid-19) constitue une « urgence sanitaire mondiale », ainsi qu'à la déclaration subséquente de l'état de crise sur base de l'article 32 paragraphe 4 de la Constitution luxembourgeoise par règlement grand-ducal du 18 mars 2020[67], la CNPD considère que l'exception prévue à l'article 9 paragraphe 2) lettre i) du RGPD est applicable en l'espèce. Ladite disposition prévoit plus précisément que le traitement de données sensibles peut être effectué lorsqu'il 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. »*

Le considérant (46) du RGPD précise dans ce contexte que certains types de traitements peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire pour suivre des épidémies et leur propagation.

En sus de l'article 9 du RGPD, le traitement de données à caractère personnel envisagé par la Direction de la santé doit se baser sur un des critères de licéité prévus à l'article 6 du RGPD. Sur base des mêmes considérations, la CNPD estime que ledit traitement est à considérer comme étant « 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 » (article 6 paragraphe (1) lettre e) du RGPD).

Le considérant (54) du RGPD énonce dans ce contexte que le *« traitement des catégories particulières de données à caractère personnel peut être nécessaire pour des motifs d'intérêt public dans les domaines de la santé publique, sans le consentement de la personne concernée. »*

La base légale de l'intérêt public sur laquelle repose donc le traitement en question[68] rend applicable l'ensemble des droits prévus par le RGPD au bénéfice des personnes concernées, à l'exclusion du droit à la portabilité. Le projet de loi n°7606 prévoit néanmoins en son article 9 paragraphe (4) que les personnes infectées ou présumées infectées ne peuvent pas s'opposer au traitement de leurs données dans le système d'information visé audit article. Par cette exclusion du droit d'opposition, il apparaît que les auteurs du projet de loi font usage de la faculté offerte par l'article 23 paragraphe (1) lettre e) du RGPD de limiter les droits des personnes pour garantir, notamment, des objectifs importants de santé publique.

Sans préjudice de ses remarques sous le point 2. concernant la durée de conservation des données, la CNPD peut a priori comprendre que cette limitation du droit d'opposition des personnes infectées, ainsi que des personnes présumées infectées et dont le test s'avère positif, est obligatoire afin de pouvoir suivre l'évolution de ce virus

[67] Il s'agit du règlement grand-ducal du 18 mars 2020 portant introduction d'une série de mesures dans le cadre de la lutte contre le Covid-19.
[68] Par l'article 6 paragraphe (1) lettre e) tout comme l'article 9 paragraphe 2) lettre i) du RGPD.

encore très peu connu par le monde scientifique, surtout qu'à *« ce stade il est prématuré d'affirmer avec certitude que la présence d'anticorps équivaut à une immunité contre l'infection, voire de se prononcer sur la durée éventuelle de cette protection. Donc, à l'heure actuelle, un résultat positif d'un test sérologique ne garantit pas une immunité. »*[69]

Néanmoins, la CNPD ne disposant pas des compétences scientifiques et épidémiologiques nécessaires, elle n'est pas en mesure d'évaluer, sans explications supplémentaires et plus précises de la part des auteurs du projet de loi, si la restriction absolue du droit d'opposition des personnes présumées infectées, mais dont le test s'avère négatif, est vraiment nécessaire dans le cadre de la lutte contre le Covid-19.

Par ailleurs, en vertu du paragraphe (2) de l'article 23 du RGPD, chaque mesure législative qui vise à limiter les droits des personnes concernées doit obligatoirement contenir un certain nombre de dispositions spécifiques y énumérées. Afin d'évaluer si le texte du projet de loi n°7606 respecte les dispositions du RGPD et répond plus particulièrement aux exigences de l'article 9 paragraphe (2) lettre i) du RGPD et dudit article 23 paragraphe (2) du RGPD, la CNPD analysera successivement les finalités du traitement et les catégories de données à caractère personnel (1.), la durée de conservation des données (2.), les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites (3.), ainsi que le droit des personnes d'être informées (4.).

1. Quant aux finalités du traitement et aux catégories de données à caractère personnel

L'article 9 paragraphe (1) du projet de loi n°7606 énumère quatre différentes finalités poursuivies par la mise en place du système d'information dont la Direction de la santé est à considérer comme responsable du traitement conformément au sens de l'article 4 point 7) du RGPD. En vertu de l'article 5 paragraphe (1) lettre b) du RGPD, les finalités d'un traitement de données doivent être déterminées, explicites et légitimes. La CNPD considère que les finalités, telles que décrites actuellement à l'article 9 du projet de loi n°7606, peuvent paraître assez larges, ce qu'elle peut a priori comprendre vu que les conséquences et le développement futur du Covid-19 n'ont pas encore pu être analysés en détail par la Direction de la santé. Néanmoins, au vu de l'ampleur du traitement et de la sensibilité des données qui y seront traitées, la Commission nationale rappelle que ces finalités doivent s'entendre strictement et que tout usage des données qui ne s'inscrirait pas dans celles-ci ne respecterait pas le principe de la limitation des finalités inscrit dans le RGPD.

En ce qui concerne les catégories de données à caractère personnel, la CNPD s'interroge sur les catégories de personnes concernées dont les données sont traitées. La stratégie de test liée au Covid-19 présentée par Madame la Ministre de la Santé le 22 mai 2020[70] comporte trois différentes manières dont les tests de diagnostic PCR[71] sont utilisés au Luxembourg : de manière réactive en présence de symptômes, de manière active au profit de certaines catégories de personnes particulièrement à risque, ainsi que de manière préventive par échantillons représentatifs (« cluster prevalence studies ») pour accompagner le déconfinement.

[69] Communiqué de presse du 22 mai 2020 du Ministère de la Santé et du Ministère de l'Enseignement supérieur et de la recherche : « COVID-19 - Une stratégie de test ambitieuse et au service de la santé publique », disponible sous : https://gouvernement.lu/dam-assets/documents/actualites/2020/05-mai/Communique-de-presse-depistage-2252020-.pdf.

[70] Communiqué de presse du 22 mai 2020 du Ministère de la Santé et du Ministère de l'Enseignement supérieur et de la recherche : « COVID-19 - Une stratégie de test ambitieuse et au service de la santé publique », disponible sous : https://gouvernement.lu/dam-assets/documents/actualites/2020/05-mai/Communique-de-presse-depistage-2252020-.pdf.

[71] Test de diagnostic (qRT-PCR) (real-time polymerase chain reaction) utilisé au Luxembourg et reposant sur un prélèvement par écouvillon réalisé au niveau nasal (naso-pharyngé) ou par la bouche (oro-pharyngé), à la recherche du matériel génétique du virus à partir du prélèvement.

Selon la compréhension de la CNPD de la configuration du système d'information, ce dernier contiendra les données relatives à deux différentes catégories de personnes concernées :

- Les personnes infectées, donc celles qui ont été testées positives au virus SARS-CoV 2, soit suite à un test prescrit par un médecin en présence de symptômes, soit suite à un test ayant eu lieu de manière active au profit de certaines catégories de personnes particulièrement à risque ou de manière préventive pour accompagner le déconfinement (les « cluster prevalence studies », le projet d'étude CON-VINCE et le « large scale testing »).

- La CNPD comprend qu'en combinant les dispositions de loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique, ainsi que l'article 9 paragraphe (2) du projet de loi n°7606, les médecins, les médecins-dentistes, les responsables de laboratoires d'analyses médicales, les établissements hospitaliers, les structures d'hébergement et les réseaux de soins sont obligés de transmettre les données relatives aux personnes infectées ou présumées infectées au Covid-19 à la Direction de la santé. Néanmoins, pour des raisons de clarté, elle propose d'énumérer de manière exhaustive les différentes sources de données dans le corps du texte de l'article 9 paragraphe (2) du projet de loi n°7606.

- Les personnes présumées infectées, c'est-à-dire celles visées par une des situations prévues à l'article 2 point 4[72] du projet de loi n°7606. Dans ce contexte, la CNPD se pose une question concernant le système du « contact tracing » qui, à l'heure actuelle, est effectué de manière manuelle au Luxembourg. Il ressort des explications contenues sur le site du gouvernement luxembourgeois dédié au Corona virus[73] que l'objectif poursuivi par ledit système de traçage est de s'assurer que les personnes qui ont eu des contacts à haut risque avec une personne dont l'infection est confirmée, donc les personnes présumées infectées, se mettent en auto-quarantaine afin de tenter de rompre la chaine de transmission du virus.

  La Commission nationale se demande néanmoins quelle est la source des données à caractère personnel des personnes présumées infectées et comment celles-ci auront connaissance de leur obligation de se mettre en quarantaine. Est-ce que la personne infectée communique les données d'identification (nom, prénom, n° de téléphone, etc.) des personnes présumées infectées à la Direction de la santé qui les insérera dans le système d'information et les contactera par la suite ? Ou est-ce que, par contre, la personne infectée contactera directement les personnes présumées infectées, ces dernières étant dans ce cas obligées de se manifester de leur propre gré auprès de la Direction de la santé qui insérera qu'à ce moment-là leurs données dans le système d'information afin de pouvoir les suivre?

  Dans le cas de figure où la source est la personne infectée qui transmet les données à la Direction de la santé, la CNPD constate que cette source n'est pas énumérée au paragraphe (2) de l'article 9 du projet de loi. Le cas échéant, il y aurait lieu de rajouter au texte la personne infectée comme source, tout comme il faudrait rajouter,

[72] Visant les différentes situations quand une personne devient une « personne présumée infectée ».
[73] https://coronavirus.gouvernement.lu/fr/citoyens.html.

le cas échéant, le numéro de téléphone à la liste des données qui peuvent être traitées, dans la mesure où cette donnée est la plus efficace et la plus rapide pour contacter les personnes.

La CNPD part de l'hypothèse que les données de tous les individus dont le test a été négatif, hormis la catégorie des personnes présumées infectées, ne sont pas transmises à la Direction de la santé par les établissements hospitaliers, les structures d'hébergement et les réseaux de soins et ne devraient, a fortiori, pas se retrouver dans le système d'information. Au cas où le système d'information contiendra néanmoins lesdites données, la Commission nationale se demande quelle serait la finalité poursuivie par ce traitement. A priori, elle est d'avis qu'aucune des finalités mentionnées à l'article 9 paragraphe (1) du projet de loi n°7606 ne permet l'enregistrement et la conservation dans le système d'information des données d'individus dont le test a été négatif (hormis de nouveau la catégorie des personnes présumées infectées). Si la finalité poursuivie est la réalisation d'études scientifiques, statistiques et/ou d'appui à la politique, et dans la mesure où il ne serait pas possible de réaliser ces traitements à partir de données anonymisées, la CNPD estime que dans ces hypothèses précises une collecte de données pseudonymisées devrait s'avérer suffisante.

Sous ces conditions, la CNPD estime que la liste des catégories de données à caractère personnel énumérées ci-dessus[74] n'est pas excessive au regard des finalités du traitement et respecte le principe de minimisation des données qui doit conduire à ne collecter que les données strictement nécessaires (article 5 paragraphe (1) lettre c) du RGPD). Par ailleurs, ladite liste de données à transférer (en plus du numéro de téléphone, le cas échéant) par les établissements hospitaliers, les structures d'hébergement et les réseaux de soins (en plus de la personne infectée comme source, le cas échéant) à la Direction de la santé doit être considérée comme exhaustive et ne pourra pas excéder les catégories de données y mentionnées.

2. Quant à la durée de conservation

L'article 5 paragraphe (1) lettre (e) du RGPD prévoit que 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 ». Il ressort par ailleurs du considérant (45) du RGPD que lorsque 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, il devrait appartenir au droit de l'Union ou au droit d'un État membre d'établir, entre autres, la durée de conservation des données. De plus, comme déjà susmentionné, l'article 5 paragraphe (1) lettre (b) du RGPD prévoit que 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 ».

Ainsi, la durée de conservation doit être déterminée en fonction de l'objectif ayant conduit à la collecte des données en cause. Une fois cet objectif atteint, ces données devraient être supprimées ou anonymisées (afin notamment de produire des statistiques).

[74] Nom, prénom, adresse, date de naissance, diagnostic médical, date des 1ers symptômes et date du diagnostic médical, date de prélèvement et origine du prélèvement, pays où la maladie a été contractée et la source d'infection si connue.

L'article 9 paragraphe (5) du projet de loi n°7606 dispose que les données à caractère personnel des personnes infectées ou présumées infectées seront conservées dans le système d'information sous une forme permettant l'identification des personnes pendant *« la durée nécessaire pour prévenir et combattre le Covid-19 et les données sont anonymisées au plus tard six mois après que la loi cesse de produire ses effets. »*

A priori, la loi en projet sous examen entrera en vigueur le lendemain de sa publication au Journal officiel du Grand-Duché de Luxembourg pour une durée d'un mois (article 13 du projet de loi n°7606). Les auteurs du projet de loi expliquent dans l'exposé des motifs que la particularité du projet de loi repose sur son applicabilité dans le temps et qu'elle produira des effets a priori uniquement du 25 juin 2020, fin de l'état de crise, au 25 juillet 2020.

Dans le commentaire de l'article 13 du projet de loi il est précisé que *« la situation sanitaire en relation avec la propagation du Covid-19 est en constante évolution ce qui explique la durée d'application limitée de la présente loi. »* La Commission nationale comprend dès lors que l'état de la crise sanitaire sera réévalué avant le 24 juillet 2020 et en fonction des résultats, elle suppose que la Chambre des députés pourra, le cas échéant, décider de prolonger l'applicabilité de la loi en cause.

Il ressort de ce qui précède qu'il y a un double délai de conservation des données : le premier délai étant celui de la fin d'applicabilité de la loi (a priori le 24 juillet 2020 mais en fonction des circonstances, ce délai pourrait être étendu comme susmentionné) et le deuxième délai se situe six mois après la fin du premier délai.

Le commentaire de l'article 9 du projet de loi n°7606 précise dans ce contexte qu'*« eu égard aux finalités du système d'information, la durée de conservation des données nominatives contenues dans le système est limitée à la durée de la gestion de la pandémie, augmentée d'une durée de six mois pour traiter d'éventuelles demandes de traitement de données provenant d'autorités de santé étrangères ou européennes ainsi que pour traiter d'éventuelles demandes liées à la recherche scientifique, historique ou à des fins statistiques. »*

La Commission nationale tient à souligner tout d'abord qu'elle ne dispose pas de l'expertise scientifique et épidémiologique nécessaire, afin d'évaluer si la conservation même des données dans le système d'information des personnes présumées infectées, mais dont le test s'avère négatif, est vraiment nécessaire dans le cadre de la lutte contre le Covid-19. En l'absence d'explications plus précises par les auteurs du projet de loi, elle ne peut pas apprécier si d'éventuels argumentations d'experts scientifiques et épidémiologiques permettent de justifier pourquoi ces données devraient être conservées pendant un certain laps de temps.

Au regard du RGPD, il est nécessaire et primordial de définir une durée de conservation des données au sein du système d'information de la Direction de la santé qui soit proportionnée au regard de la finalité poursuivie. Partant, il est nécessaire de définir des critères objectifs permettant de justifier une durée de conservation adéquate.

ANNEXES

5

Au risque de se répéter, la CNPD n'étant pas experte en matière de santé et de gestion d'épidémies, il est difficile pour elle d'évaluer s'il est proportionné, afin de combattre l'expansion du Covid-19, que les données à caractère personnel des personnes infectées et présumées infectées seront conservées dans le système d'information pendant un nombre déterminé de mois. Elle se demande néanmoins quelles sont les raisons sanitaires et/ou scientifiques qui ont amené les auteurs du projet de loi à insérer dans l'article 9 paragraphe (5) du RGPD une durée de conservation spécifique de 6 mois après que la future loi cessera de produire ses effets.

A titre de comparaison, la loi française n°2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions contient une disposition a priori similaire au texte proposé par le législateur luxembourgeois. En effet, l'article 11 dispose *« qu'aux seules fins de lutter contre la propagation de l'épidémie de covid-19 et pour la durée strictement nécessaire à cet objectif ou, au plus, pour une durée de six mois à compter de la fin de l'état d'urgence sanitaire déclaré par l'article 4 de la loi n°2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, des données à caractère personnel concernant la santé relatives aux personnes atteintes par ce virus et aux personnes ayant été en contact avec elles peuvent être traitées et partagées, le cas échéant sans le consentement des personnes intéressées, dans le cadre d'un système d'information créé par décret en Conseil d'État et mis en œuvre par le ministre chargé de la santé. »*

Or, l'alinéa 2 de l'article 11 précité contient une précision importante, dans la mesure où *« les données à caractère personnel collectées par ces systèmes d'information à ces fins ne peuvent être conservées à l'issue d'une durée de trois mois après leur collecte »*. Ainsi, même si le système français en lui-même pourra fonctionner jusqu'au plus tard six mois après la fin de l'état d'urgence sanitaire, les données à caractère personnel devraient régulièrement être supprimées, voir anonymisées, trois mois après qu'elles ont été collectées.

En Belgique, l'arrêté royal n°25 du 28 mai 2020 modifiant l'arrêté royal n°18 du 4 mai 2020 portant création d'une banque de données auprès de Sciensano dans le cadre de la lutte contre la propagation du coronavirus COVID-19, est entré en vigueur le 5 juin 2020. Comme l'arrêté royal n°18 du 4 mai 2020 cessait déjà ses effets le 4 juin 2020, il a été décidé de le proroger jusqu'au 30 juin 2020. Dans le rapport au roi, la Ministre des Affaires sociales et de la Santé publique belge a précisé que *« le délai pour l'effacement des données à caractère personnel serait ajusté en conséquence (le 5 juillet 2020 au lieu du 9 juin 2020) »*, soit une durée de conservation des données de cinq jours après la fin de validité de l'arrêté en cause.

Pour conclure, la CNPD ne peut que constater que les législateurs des pays voisins du Luxembourg ont opté dans ce contexte pour des durées de conservation beaucoup plus courtes. Or, comme susmentionné, la Commission nationale n'a pas les éléments et explications nécessaires à sa disposition pour se prononcer sur la proportionnalité d'un délai de conservation des données des personnes infectées et présumées infectées de six mois après que la loi cessera de produire ses effets.

Afin de garantir que les données ne soient pas conservées plus longtemps que nécessaire, des délais devraient être fixés soit pour leur effacement, soit pour un examen périodique. Ainsi, une alternative serait de prévoir qu'en fonction de l'évolution du Covid-19, la pertinence d'une durée de conservation a priori plus brève que six mois, fasse l'objet d'une évaluation régulière, surtout qu'à l'heure actuelle, il n'est pas possible de prédire combien de fois et pendant quel laps de temps l'applicabilité de la loi en projet sera prolongée.

3. Quant aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites

La Commission nationale rappelle que, quel que soit le contexte d'urgence, des garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données à caractère personnel doivent être apportées. L'encadrement des accès à des données de santé est essentiel dans ce contexte au regard des exigences prévues par l'article 9 paragraphe 2 lettre i) du RGPD.

En vertu de l'article 9 paragraphe (3) du projet de loi sous revue, *« seuls les médecins et professionnels de la santé, nommément désignés et habilités dans le cadre de la présente loi par le directeur de la santé ou de son délégué pour détecter, évaluer, surveiller et combattre le Covid-19 sont autorisés à accéder aux données relatives à la santé des personnes infectées ou présumées infectées. »* Ledit paragraphe continue en limitant l'accès aux données relatives à la santé dans la stricte mesure où il *« est nécessaire à l'exécution des missions légales ou conventionnelles qui leur sont confiées pour prévenir et combattre le Covid-19. »*

Etant donné le caractère sensible des données relatives à la santé, la Commission nationale ne peut qu'approuver que le cercle des personnes pouvant accéder aux données liées à la santé et le contexte dans lequel ils y accèdent est circonscrit. Il ressort de l'article 9 paragraphe (3) du projet de loi que toutes les personnes que le directeur de la santé peut habiliter à accéder au système d'information sont soumises au secret professionnel prévu à l'article 458 du Code pénal, comme il est par ailleurs exigé par l'article 9 paragraphe 2 lettre i) précité du RGPD.

L'article 9 paragraphe (5) du projet de loi requiert en plus que les *« données sont traitées dans des conditions permettant d'en garantir la sécurité, la confidentialité et l'intégrité. »* Au vu de la nature et du volume des données traitées ainsi que des risques pour les personnes en cas d'atteinte à la sécurité des données, la CNPD estime incontournable que des mesures de sécurité technique et organisationnelle adéquates soient mises en place afin de garantir un niveau de sécurité à l'état de l'art du secteur de la santé.

A cet égard, la CNPD tient à souligner l'importance de l'obligation de sécurité prévue à l'article 5 paragraphe (1) lettre f) et à l'article 32 du RGPD, exigeant que des mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, soient mises en place. Elle considère que la mise en œuvre du traitement de données à caractère personnel contenues dans le système d'information devra en particulier garantir le recours à une authentification forte des personnes ayant accès et ledit système devrait être doté d'un traçage (journalisation)

individuel des accès pendant une durée de cinq ans à partir de l'enregistrement du log, ce qui constitue une garantie supplémentaire en matière de protection des données à caractère personnel. Il est également primordial que les données soient détruites irréversiblement après l'expiration du délai de conservation.

4. Quant aux droits des personnes concernées

Le paragraphe (4) de l'article 9 du projet de loi précise que *« les droits des personnes concernées prévus par le règlement général sur la protection des données (UE) 2016/679 s'exercent auprès de la Direction de la santé »*. Pour ce qui est de la limitation du droit d'opposition, la CNPD renvoie à ses observations ci-avant.

En vertu des articles 13 et 14 du RGPD, le responsable du traitement est obligé de fournir aux personnes concernées certaines informations lorsque des données à caractère personnel sont collectées directement auprès d'elles ou indirectement à travers un tiers. Une information précise et adaptée devra donc être apportée aux personnes concernées dans un contexte sanitaire particulier.

Ainsi, en vertu de l'article 14 du RGPD, la Direction de la santé est obligée de fournir ces informations à la personne infectée, ces données provenant a priori d'un tiers (les établissements hospitaliers, les structures d'hébergement et les réseaux de soins). En ce qui concerne les données à caractère personnel relatives aux personnes présumées infectées dans le contexte du « contact tracing », il n'est pas clair si cette collecte s'effectue de manière directe par la Direction de la santé ou de manière indirecte (par exemple via la personne infectée elle-même). Dans les deux hypothèses, le droit à l'information desdites personnes est à respecter par la Direction de la santé.

Finalement, la CNPD tient à préciser qu'au moment où une personne effectue un test, elle devrait en principe déjà être informée du fait qu'en cas de résultat positif, ses données à caractère personnel seront transférées vers la Direction de la santé et y enregistrées dans leur système d'information.

Ainsi décidé à Esch-sur-Alzette en date du 8 juin 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

Avis complémentaire relatif au projet de loi n°7606 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre le virus SARS-CoV-2 (COVID-19) et modifiant 1. la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2. la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments.

(Délibération n°14/2020 du 16 juin 2020)

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 ».*

Suite aux amendements adoptés par la Commission de la Santé et des Sports en date du 11 juin 2020 concernant le projet n°7606 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre le virus SARS-CoV-2 (COVID-19) et modifiant 1. la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2. la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments (ci-après le « projet de loi »), la CNPD entend encore formuler, en sus de son avis initial n°13/2020 du 8 juin 2020, les observations qui suivent.

Par l'amendement 3 du projet de loi n°7606, les auteurs ont notamment inséré un paragraphe 2 nouveau à l'article 5 dudit projet et qui concerne les activités de transport de personnes par moyen collectif dans le cadre d'un voyage organisé. Ainsi, afin de suivre l'évolution de la propagation du Covid-19 dans le cadre d'un voyage organisé, l'exploitant d'un moyen collectif de transport de personnes *« est tenu de transmettre dans la mesure du possible, sur demande, au médecin de la Direction de la santé ou aux professionnels de la santé habilités dans le cadre de la présente loi par le directeur de la santé les nom, prénom, numéro de téléphone et adresse électronique des personnes qui ont subi une exposition à haut risque en raison d'une des situations visées à l'article 2, point 4°. » Le commentaire de l'amendement ajoute que les données relatives aux passagers à haut risque d'être infectés et qui sont adressées à la Direction de la santé sur demande précisent en outre « le moyen, la date et l'heure du transport et, le cas échéant, la voiture et le siège occupés par le cas index. »*

Il en découle, comme le précisent d'ailleurs les auteurs de l'amendement, que l'exploitant d'un tel moyen de transport dispose déjà à la base des données d'identification des voyageurs ayant utilisé le moyen de transport concerné et dans lequel une ou plusieurs personnes infectées ont pu être localisées. Or, tandis que la finalité initiale de cette collecte de données à caractère personnel des passagers est plutôt l'organisation d'un voyage, la CNPD comprend que les auteurs de l'amendement visent une autre finalité par cette obligation de transférer sur demande les données des passagers par l'exploitant d'un moyen collectif de transport de personnes à la Direction de la santé : mettre en place un système de traçage pour identifier le plus tôt possible toute personne à risque ou à haut risque d'être infectée afin de mettre en œuvre les précautions nécessaires (comme une mise en quarantaine) et de prévenir ainsi la dissémination de l'infection par ces personnes à leur tour contagieuses.

La CNPD ne remet pas en cause le principe que ce traitement soit nécessaire afin de poursuivre la finalité précitée et afin de fournir à la Direction de la santé les moyens pour contacter le plus rapidement possible les passagers potentiellement exposés.

Néanmoins, elle tient à formuler deux remarques dans ce contexte :

- Le commentaire de l'article précise que les termes « exploitant d'un moyen collectif de transport de personnes » concernent les « transports terrestres (bus à longues distances, en particulier à l'occasion des congés d'été, trains à longue distance), aériens et fluviaux ». Or, la CNPD se demande plus particulièrement ce qu'il faut entendre par « voyage organisé ». Est-ce que les voyages individuels et « non organisés » (comme par exemple un simple vol aller-retour de l'aéroport de Luxembourg ou un voyage en train par le TGV depuis la Gare de Luxembourg-ville) ne sont pas visés par la disposition en cause et que donc, même si on est en présence d'un exploitant d'un moyen collectif de transport de personnes, cette obligation de transmettre sur demande des données des passagers à la Direction de la santé ne s'appliquerait pas dans cette hypothèse ?

- Comme susmentionné, afin de pouvoir procéder au transfert du nom, prénom, numéro de téléphone et adresse électronique des personnes qui ont subi une exposition à haut risque à la Direction de la santé, les exploitants d'un moyen collectif de transport de personnes doivent au préalable déjà être en possession desdites données. Le commentaire de l'amendement en cause précise à cet égard que *« le passager visé par cette mesure doit donner son consentement au préalable. »*

  Néanmoins, la CNPD est d'avis qu'il ressort implicitement de l'utilisation des mots *« est tenu de transmettre »* dans le corps du texte de l'article 5 paragraphe (2) du projet de loi n°7606 tel qu'amendé, que ce n'est pas une simple option pour les exploitants en fonction de l'accord du passager de transmettre sur demande à la Direction de la santé les données précitées, mais que, par contre, ils sont obligés de procéder audit transfert. Par ailleurs, elle doute que le consentement des passagers respecterait, le cas échéant, toutes les conditions prévues par le RGPD pour être licite, notamment en ce qui concerne son caractère libre.

Concernant de manière générale la durée de conservation des données à caractère personnel, la CNPD renvoie à ses remarques y relatives formulées dans son avis précité du 8 juin 2020 sur le projet de loi n°7606. Ayant trait à la durée de conservation spécifique des données à caractère personnel des passagers auprès de l'exploitant, les auteurs précisent dans le commentaire de l'amendement qu'elle « ne doit pas être supérieur à 14 jours (durée d'incubation maximale, en cas de contamination pendant le voyage, le passager contaminé sera déjà malade lui-même) ; au terme de ce délai, elles sont détruites. » La CNPD ne peut que soutenir ce délai de suppression court qui paraît être proportionné par rapport à la finalité poursuivie par le traitement en cause, c'est-à-dire, envoyer les données relatives aux passagers à haut risque d'être infectés à la Direction de la santé pour s'assurer qu'ils se mettent en auto-quarantaine afin de tenter de rompre la chaine de transmission du virus. Or, pour des raisons de clarté et de sécurité juridique, la CNPD suggère d'insérer cette précision sur la durée de conservation des données dans le corps du texte de l'article 5 paragraphe (2) du projet de loi n°7606 amendé.

Ainsi décidé à Esch-sur-Alzette en date du 16 juin 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

ANNEXES

5

Avis relatif au projet de règlement grand-ducal portant fixation du siège de la Commission nationale pour la protection des données.

(Délibération n°15/2020 du 26 juin 2020)

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 ».*

Par lettre en date du 11 juin 2020, 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 (ci-après le « projet de règlement grand-ducal »).

L'entrée en application du RGPD a été accompagnée par une loi de mise en œuvre, 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. L'article 3 de cette loi prévoit que le siège de la CNPD est fixé par règlement grand-ducal. Le règlement grand-ducal du 1er août 2018 portant fixation du siège de la Commission nationale pour la protection des données avait consacré que le maintien du siège à Esch-sur-Alzette était la solution adéquate pour la situation de la CNPD.

L'exposé des motifs du projet de règlement grand-ducal mentionne de manière pertinente qu'avec l'entrée en application du RGPD, de la loi de mise en œuvre et de la loi du 1er août 2018 relative à la protection des données en matière pénale ainsi qu'en matière de sécurité nationale, les ressources humaines et financières de la CNPD ont été augmentées substantiellement afin de répondre à ses nouvelles compétences et missions, ainsi qu'à ses nouveaux pouvoirs. Les capacités maximales en terme de places de bureaux pouvant être mis à disposition par le Fonds Belval ont toutefois été atteintes.

La CNPD a par conséquent elle-même recherché des locaux correspondant à ses besoins situés dans le quartier du Belval, mais relevant dès à présent de la commune de Sanem, et non plus de celle d'Esch-sur-Alzette. Le projet

de règlement grand-ducal sous avis s'inscrit dans la mise en œuvre de l'article 3 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 en ce qu'il est nécessaire de changer la fixation du siège de la CNPD d'Esch-sur-Alzette à Sanem.

Néanmoins, comme les nouveaux locaux de la CNPD se trouvent plus précisément sur le territoire de Belvaux, une des quatre localités de la commune de Sanem, la CNPD propose de préciser à l'article 1er du projet de règlement grand-ducal que le siège de la Commission nationale pour la protection des données est fixé dans la « Commune de Sanem, localité de Belvaux », au lieu de simplement « Sanem ».

Par ailleurs, l'article 2 du projet de règlement grand-ducal prévoit que le *« règlement grand-ducal du 1er août 2018 portant transfert du siège de la Commission nationale pour la protection des données est abrogé. »* Or, le texte à abroger était intitulé *« règlement grand-ducal du 1er août 2018 portant fixation du siège de la Commission nationale pour la protection des données »*. Ainsi, la CNPD recommande de remplacer le mot « transfert » par « fixation ».

Ainsi décidé à Esch-sur-Alzette en date du 26 juin 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

ANNEXES

5

Avis relatif au projet de loi n°7622 1°portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 ; 2° modifiant 1) la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2) la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments ; 3° abrogeant 1) la loi du 24 juin 2020 portant introduction d'une série de mesures concernant les activités sportives, les activités culturelles ainsi que les établissements recevant du public, dans le cadre de la lutte contre la pandémie Covid-19; 2) la loi du 24 juin 2020 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre la pandémie Covid-19 et modifiant la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments.

(Délibération n°16/2020 du 8 juillet 2020)

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 ».*

En date du 7 juillet 2020, Madame la Ministre de la Santé a saisi la Commission nationale à se prononcer sur le projet de loi n°7622 1°portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 ; 2° modifiant 1) la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2) la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments ; 3° abrogeant 1) la loi du 24 Juin 2020 portant introduction d'une série de mesures concernant les activités sportives, les activités culturelles ainsi que les établissements recevant du public, dans le cadre de la lutte contre la pandémie Covid-19; 2) la loi du 24 Juin 2020 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre la pandémie Covid-19 et modifiant la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments (ci-après : « le projet de loi n°7622 »).

Il ressort de l'exposé des motifs qu'afin de faciliter la lisibilité des mesures de lutte contre la pandémie Covid-19, le présent projet de loi vise à fusionner en un seul texte de loi, d'un côté la loi du 24 juin 2020 portant introduction

d'une série de mesures concernant les activités sportives, les activités culturelles ainsi que les établissements recevant du public, dans le cadre de la lutte contre la pandémie Covid-19, et d'un autre côté la loi du 24 juin 2020 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre la pandémie Covid-19 et modifiant la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments (ci-après : « la loi du 24 juin 2020 »).

La CNPD renvoie dans ce contexte à ses avis n°13/2020 du 8 juin 2020 et n°14/2020 du 16 juin 2020 relatifs au projet de loi n°7606 devenu la loi du 24 juin 2020 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre la pandémie Covid-19 et modifiant la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments. Elle salue que la majorité de ses remarques y émises a été prise en compte par les auteurs du projet de loi n°7606.

Elle constate que les auteurs du projet de loi n°7622 sous examen ont repris quasi l'intégralité des dispositions en matière de protection des données prévues par la loi du 24 juin 2020. En effet, l'article 5 du projet de loi n°7622 reprend en majeure partie les dispositions de l'article 4 de la loi du 24 juin 2020 concernant le traçage des contacts, tandis que l'article 10 dudit projet de loi reprend les dispositions de l'article 8 de la loi du 24 juin 2020 sur la création d'un système d'information par le directeur de la santé.

Les articles 5 paragraphe (1) et 10 paragraphe (3) du projet de loi n°7622 font l'objet de rajouts en ce sens qu'à côté du directeur de la santé ou son délégué, les fonctionnaires ou employés désignés à cet effet par ledit directeur sont autorisés dans le cadre du traçage des contacts de traiter les données des personnes infectées ou à haut risque d'être infectées, respectivement d'accéder à leurs données contenues dans le système d'information précité. Il ressort du commentaire de l'article 10 du projet de loi n°7622 qu'en raison de l'augmentation des nouvelles infections ces derniers jours et corrélativement de la charge de travail de l'équipe du traçage de contacts de la direction de la santé, ainsi que le manque *« de médecins et professionnels de santé en nombre suffisant pour effectuer ces travaux, il est proposé de donner la possibilité au directeur de la santé de recourir, pour l'exécution de ces tâches, également à des fonctionnaires ou employés désignés par lui à cet effet. »*

Il est par ailleurs précisé à l'article 10 paragraphe (3) du projet de loi sous avis que tous ceux qui peuvent accéder au système d'information, donc aussi les fonctionnaires ou employés désignés à cet effet par le directeur de la santé, sont soumis au secret professionnel et que les dispositions prévues à l'article 458 du code pénal sont applicables. Sous ces conditions restrictives, que donc le non-respect du secret professionnel dans ce contexte est soumis aux sanctions pénales prévues à l'article 458 du code pénal, la CNPD estime que les accès supplémentaires au système d'information apparaissent légitimes.

Ainsi décidé à Esch-sur-Alzette en date du 8 juillet 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

ANNEXES

5

Avis relatif au projet de loi n°7543 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale et au projet de règlement grand-ducal portant : 1° fixation des conditions et modalités de l'épreuve spéciale de l'examen-concours pour l'admission au stage pour les catégories de traitement A et B et le groupe de traitement C1 du cadre policier ; 2° fixation des conditions et modalités de recrutement pour le groupe de traitement C2 du cadre policier ; 3° portant modification du règlement grand-ducal modifié du 30 septembre 2015 fixant les conditions et modalités d'inscription et d'organisation des examens-concours d'admission au stage dans les administrations et services de l'État.

(Délibération n°17/2020 du 17/07/2020)

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 ») ainsi qu'à l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention 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, 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, tandis que l'article 8 point 3° de ladite loi du 1er août 2018 se base sur l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n°2016/680 précitée en prévoyant que la CNPD *« conseille la Chambre des députés, 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 des données personnelles ».*

Par courrier en date du 25 mars 2020, Monsieur le Ministre de la Sécurité intérieure a invité la Commission nationale à se prononcer sur le projet de de règlement grand-ducal portant : 1° fixation des conditions et modalités de l'épreuve spéciale de l'examen-concours pour l'admission au stage pour les catégories de traitement A et B et le

groupe de traitement C1 du cadre policier ; 2° fixation des conditions et modalités de recrutement pour le groupe de traitement C2 du cadre policier ; 3° portant modification du règlement grand-ducal modifié du 30 septembre 2015 fixant les conditions et modalités d'inscription et d'organisation des examens-concours d'admission au stage dans les administrations et services de l'État (ci-après le « projet de règlement grand-ducal »).

Ce projet de règlement grand-ducal s'inscrit, tout comme le projet de loi n°7543 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale (ci-après le « projet de loi »), dans le cadre d'une réforme de l'accès aux carrières policières et de la formation des fonctionnaires stagiaires du cadre policier.

Si le projet de règlement grand-ducal a notamment pour objet de fixer les conditions requises pour l'admission au stage pour les catégories de traitement A et B et le groupe de traitement C1 du cadre policier, il y a lieu de constater que le projet de loi prévoit également qu'afin d'être admis au stage les candidats doivent *« disposer des qualités morales nécessaires à l'exécution d'une des fonctions du cadre policier »*[75]. Afin de déterminer si les candidats remplissent cette condition, une enquête de moralité est effectuée par la Police grand-ducale.

Dans la mesure où le projet de règlement grand-ducal et le projet de loi traitent tous deux des conditions d'admission au stage pour l'une des fonctions du cadre policier, la Commission nationale s'autosaisit pour aviser le projet de loi ensemble avec le projet de règlement grand-ducal.

I. Sur le projet de loi

1. Remarques liminaires

La Commission nationale se félicite que l'article 58 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, d'un point de vue de la sécurité juridique, constitue la base légale de l'enquête de moralité effectuée par la Police grand-ducale dans le contexte exposé ci-avant, conformément à l'article 6 paragraphe (3) du RGPD[76].

En effet, il convient de rappeler que le traitement de données à caractère personnel collectées et traitées dans le cadre de l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement doit reposer sur une base légale conformément à l'article 6 paragraphe (3) du RGPD, lu ensemble avec son paragraphe (1) lettres c) et e)[77] qui dispose que : « Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par :

a. le droit de l'Union; ou
b. 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 public ou relevant de l'exercice

[75] Article 1 du projet de loi ayant pour objet de modifier l'article 58 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.
[76] Il y a lieu de préciser que 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 n'a pas vocation à s'appliquer dans le cas présent alors que les traitements mis en œuvre par la Police grand-ducale le sont à des fins de recrutements.
[77] L'article 6, paragraphe (1), lettres c) et e) dispose que : *« Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : (…) c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; (…) e) 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; (…) »*

de l'autorité publique dont est investi le responsable du traitement. 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. »

Cet article 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 définis soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis.

De plus, 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. […] ».*

En vertu des dispositions précitées, ces bases légales devraient établir des dispositions spécifiques visant à déterminer, entre autres, les types de données traitées, les personnes concernées, les entités auxquelles les données peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement. Le considérant (41) du RGPD énonce encore 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 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. ».* Au niveau national une base juridique peut dès lors constituer un acte législatif ou réglementaire, ce qui est le cas en l'espèce du projet de loi et du projet de règlement grand-ducal sous examen.

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 européenne des droits de l'Homme[78], que si elle repose sur un article du droit national qui présente certaines caractéristiques. L'expression « prévue par la loi » implique donc selon la jurisprudence de la Cour européenne des droits de l'Homme que la législation interne doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention[79]. La législation interne doit être *« accessible aux personnes concernées et prévisible quant à ses répercussions »*[80]. 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 »*[81] ainsi que *« Le degré de précision requis de la "loi" à cet égard dépendra du sujet en question. »*[82].

Afin de remplir ces critères d'accessibilité et de prévisibilité de la « loi », d'une part, et ainsi limiter d'éventuels comportements arbitraires et abusifs de la part des autorités publiques, d'autre part, le droit national peut donc prévoir et encadrer plus spécifiquement les traitements de données à caractère personnel effectués par de telles autorités, comme la Police grand-ducale. Cet encadrement légal serait par ailleurs un garant du principe de sécurité juridique au profit des personnes concernées, les candidats aux carrières policières. La sécurité juridique constitue même un principe général du droit de l'Union européenne, exigeant notamment qu'une réglementation entraînant des conséquences défavorables à l'égard de particuliers soit claire et précise et son application prévisible pour les justiciables. La réglementation doit permettre aux intéressés de connaître avec exactitude l'étendue des obligations qu'elle leur impose, doit leur permettre de connaître sans ambiguïté leurs droits et leurs obligations ainsi que leur permettre de prendre leurs dispositions en conséquence[83].

[78] L'article 8 paragraphe (2) de la Convention européenne des droits de l'Homme dispose que : *« Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui »*

[79] *CouEDH, Fernández Martínez c. Espagne [GC], n°56030/07, para. 117*

[80] *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.*

[81] *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.*

[82] *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.*

[83] *Voir p.ex. Cour EDH, Aurubis Balgaria du 31 mars 2011, C-546/09, points 42-43 ; Arrêt, Alfamicro c. Commission du 14 novembre 2017, T-831/14, points 155-157.*

C'est la raison pour laquelle, la Cour européenne des droits de l'Homme au sein de sa jurisprudence affirme que *« le droit interne doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par l'article 8 paragraphe 1 »*[84]. Par conséquent, la législation interne *« doit définir l'étendue et les modalités d'exercice du pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire »*[85]. La Cour de justice de l'Union européenne estime qu'en cas de limitation de la protection des données à caractère personnel ou du droit au respect de la vie privée un texte légal *« doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »*[86].

Dès lors, dans la mesure où les traitements de données mises en œuvre par la Police grand-ducale dans le cadre du projet de loi et du projet de règlement grand-ducal constituent une ingérence dans le droit au respect de la vie privée des candidats aux carrières policières, le projet de loi et le projet de règlement grand-ducal devraient encadrer plus spécifiquement de tels traitements conformément à la jurisprudence de la Cour européenne des droits de l'Homme. Cet encadrement légal serait par ailleurs un garant du principe de sécurité juridique au profit des personnes concernées, les candidats aux carrières policières. La sécurité juridique constitue même un principe général du droit de l'Union européenne, exigeant notamment qu'une réglementation entraînant des conséquences défavorables à l'égard de particuliers soit claire et précise et son application prévisible pour les justiciables. La réglementation doit permettre aux intéressés de connaître avec exactitude l'étendue des obligations qu'elle leur impose, doit leur permettre de connaître sans ambiguïté leurs droits et leurs obligations ainsi que leur permettre de prendre leurs dispositions en conséquence[87].

Par ailleurs, la protection des données à caractère personnel constitue au niveau national une matière réservée à la loi en ce qu'elle touche à la protection de la vie privée des citoyens (article 11 paragraphe (3) de la Constitution). En vertu de l'article 32, paragraphe (3), de la Constitution, dans lesdites matières réservées à la loi par la Constitution, *« le Grand-Duc ne peut prendre des règlements et arrêtés qu'en vertu d'une disposition légale particulière qui fixe, outre les objectifs, les principes et points essentiels des mesures d'exécution. »*[88].

Les éléments essentiels[89], les objectifs et les principes[90] doivent dès lors figurer dans la loi au sens stricte du terme.

Ainsi, et bien que l'enquête de moralité dispose d'une base légale, telle que prévue par l'article 58 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, la Commission nationale relève que les conditions et les modalités du traitement mis en œuvre lors de l'enquête de moralité ne sont pas précisées dans l'article 58 précité, tel que

[84] *Cour EDH, Amann c. Suisse [GC], n°27798/95 para 56.*
[85] *Ibidem. Voir également Cour EDH, Malone c. Royaume-Uni, série A n°82, du 2 août 1984, pp. 31-32, para.66 ; Cour EDH, Fernández Martínez c. Espagne CE:ECHR:2014:0612JUD005603007, 12 juin 2014 para.117 ; Cour EDH, Liberty et autres c. Royaume-Uni, n°58243/00, du 1er juillet 2008, para. 62 et 63; Cour EDH, Rotaru c. Roumanie, App. n°28341/95, 4 mai 2000, para. 57 à 59 et Cour EDH, S et Marper c. Royaume-Uni, Requêtes n°30562/04 et 30566/04, du 4 décembre 2008 para. 99. ; Dimitrov-Kazakov c. Bulgarie n°11379/03, du 10 février 2011.*
[86] *Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :2014 :238, point 54.*
[87] *Voir p.ex. Cour EDH, Aurubis Balgaria du 31 mars 2011, C-546/09, points 42-43 ; Arrêt, Alfamicro c. Commission du 14 novembre 2017, T-831/14, points 155-157.*
[88] *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.*
[89] *Arrêt de la Cour constitutionnelle - Arrêts n°00132 et 00133 du 2 mars 2018.*
[90] *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.*

modifié par l'article 1 du projet de loi, alors que cette enquête constitue une ingérence dans le droit au respect de la vie privée et le droit à la protection des données.

2. <u>Sur l'enquête de moralité</u>

La Commission nationale salue que l'enquête de moralité soit prévue par une base légale, telle que prévue à l'article 58 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale. De même qu'elle se félicite que l'article 58 précité, tel que modifié par l'article 1 du projet de loi, précise désormais les conséquences du défaut des qualités morales nécessaires à l'exécution d'une des fonctions du cadre policier. Cependant et comme exposé ci-avant certaines précisions mériteraient d'être apportées.

a. <u>Sur l'absence de définition des qualités morales requises par les candidats à l'une des fonctions du cadre policier dans la loi</u>

En effet, en l'absence de définition des qualités morales requises par le candidat à l'une des fonctions du cadre policier, il est difficile de saisir les contours et la portée de l'enquête de moralité.

En outre, l'absence de définition des qualités morales requises par les candidats à l'une des fonctions du cadre policier, qui est pourtant une des conditions essentielles à leur admission au stage, ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal. Une loi doit être suffisamment claire et précise afin de permettre aux personnes concernées de connaître l'étendue des limitations, ainsi que les conséquences éventuelles pour elles[91].

i. <u>Les principes dégagés par la jurisprudence administrative</u>

Si l'article 58 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, tel que modifié par le projet de loi, reste muet quant à la définition des notions de qualités morales, il y a lieu de relever que la jurisprudence administrative apporte des éléments de réponse quant à ce que recouvre de telles notions.

Il découle notamment des principes dégagés par la jurisprudence administrative que la moralité d'un candidat à l'une des fonctions du cadre policier s'apprécie sur base de vastes critères qui ne reposent pas uniquement sur l'appréciation des antécédents judiciaires du candidat (par exemple l'état d'esprit du candidat, son sens des responsabilités)[92]. Cela est d'ailleurs corroboré par les travaux parlementaires relatifs au projet de loi n°7045 portant réforme de la Police grand-ducale qui précisent dans le document parlementaire 7045/09[93] que : *« les policiers sont chargés d'assurer la sécurité intérieure et sont à cet effet dotés de moyens de contrainte, ce qui justifie que leurs conditions de moralité ne sont pas appréciées sur base du seul casier judiciaire ».*

[91] Voir entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06, § 228-229, 4 décembre 2015.

[92] En effet, la jurisprudence administrative précise que la notion de moralité implique une appréciation globale « *des qualités morales d'un candidat à l'examen et notamment de état d'esprit, de son sens des responsabilités, de ses capacités sociales, de son attitude relative au respect des normes du pays, étant donné que les membres de la Police grand-ducale ont justement pour mission d'assurer la sécurité intérieure en veillant au maintien de l'ordre public et au respect et à l'exécution des lois et règlements.* ». Voir en ce sens jugement du 2 avril 2019 du Tribunal administratif du Grand-Duché de Luxembourg, 4ième chambre, numéro 39804 du rôle, et jugement du 18 janvier 2019 du Tribunal administratif du Grand-Duché de Luxembourg, 4ième chambre, numéro 41619 du rôle.

[93] Pages 29 et 30.

Il ressort également de la jurisprudence administrative en la matière que l'appréciation de la moralité d'un candidat doit se faire *in concreto*[94] et relève du pouvoir discrétionnaire de la Police grand-ducale[95].

Par conséquent, dans la mesure où ce n'est pas la loi qui définit sur quels éléments portent l'enquête de moralité ou quels sont les critères ou le degré de gravité des antécédents pris en compte mais la jurisprudence administrative et ce alors que l'enquête de moralité constitue une ingérence indéniable dans le droit à la vie privée et à la protection des données des candidats, la Commission nationale estime nécessaire que l'article 58, tel que visé au projet de loi, reflète les principes dégagés par la jurisprudence administrative quant à la notion de qualité morale.

En effet, le texte actuel manque de transparence et ne permet pas au candidat de savoir quels sont les critères ou quel degré de gravité de ses antécédents, le cas échéant, sont pris en compte par la Police grand-ducale, afin d'apprécier s'il dispose des qualités morales nécessaires. Lors de cette enquête, la Police grand-ducale est-elle amenée à consulter des fichiers étatiques, des fichiers internes de la Police grand-ducale ou encore d'autres fichiers ? Une énumération des fichiers consultés, plutôt que la formule actuelle utilisée[96], permettrait au candidat d'avoir une meilleure compréhension des conditions qu'il doit remplir afin d'accéder à l'une des fonctions du cadre policier.

Par ailleurs, à titre d'exemple, il y a lieu d'attirer l'attention des auteurs du projet de loi sur le fait que la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, telle que modifiée, prévoit les modalités de l'enquête de sécurité dont font l'objet les fonctionnaires de l'État et employés de l'État affectés au Service de renseignement, afin de vérifier notamment s'ils disposent des garanties de moralité. Bien que cette loi ne définisse pas la notion de « garantie de moralité », elle est cependant plus précise en ce qui concerne les accès aux base de données consultés dans le cadre de l'enquête de sécurité et les traitements de données collectées lors d'une telle enquête (voir articles 21 à 23 de la loi précitée).

ii. Le cadre légal national comparé à celui en Belgique et en France

Dans le cadre du recrutement des policiers, il est intéressant de noter que tant la loi belge que française prévoient une condition similaire à celle requise par l'article 58 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale à savoir que le candidat à l'une des fonctions du cadre policier doit disposer des *« qualités morales nécessaires à l'exécution d'une des fonctions du cadre policier ».*

En effet, en Belgique, un candidat à un des postes du cadre opérationnel au sein de la police doit notamment *« être de conduite irréprochable et ne pas présenter de facteurs de risque qui constituent un obstacle à l'engagement à la police »*[97]. Le texte de loi belge précise en outre que les conditions précitées découlent : *« a) d'une copie certifiée conforme du casier judiciaire complet datant de moins de trois mois à la date d'introduction de la candidature ; b) d'une enquête de milieu et des antécédents, comprenant notamment un entretien avec le candidat au domicile et au lieu de résidence éventuel de celui-ci, diligentée par le corps de police locale ; c) de toutes les informations*

[94] La jurisprudence énonce que : *« le pouvoir de nomination n'est pas tenu à ne prendre en considération que des faits qualifiés pénalement en rapport direct avec la fonction à exercer, de même qu'il n'est pas lié par l'appréciation de certains faits faite par des juges correctionnels, en ce que l'objectif de son intervention est différent de celui de ces derniers qui ont à sanctionner des comportements répréhensibles au sens de la loi, alors que le ministre doit veiller, par une appréciation in concreto, au respect des conditions fixées par la loi dans le chef des candidats policiers notamment du point de vue de leur moralité. ».* Voir en ce sens jugement du 2 avril 2019 du Tribunal administratif du Grand-Duché de Luxembourg, 4ième chambre, numéro 39804 du rôle, et jugement du 18 janvier 2019 du Tribunal administratif du Grand-Duché de Luxembourg, 4ième chambre, numéro 41619 du rôle.

[95] Jugement du 2 avril 2019 du Tribunal administratif du Grand-Duché de Luxembourg.

[96] L'article 58 de la loi modifiée du 18 juillet 2018 prévoit que la Police grand-ducale *« peut consulter les fichiers qui lui sont légalement accessibles et pour autant que cette consultation est pertinente quant à la finalité recherchée ».*

[97] Article 12, 3° de la Loi du 26 avril 2002 relative aux éléments essentiels du statut des membres du personnel des services de police et portant diverses autres dispositions relatives aux services de police.

disponibles transmises par les services de renseignement et de sécurité et par l'Organe de coordination pour l'analyse de la menace ; d) de toutes les informations disponibles relatives aux sanctions administratives communales imposées pour une infraction mixte ; e) des données judiciaires, communiquées par les services de police, moyennant autorisation des autorités judiciaires compétentes ; f) des autres données et informations validées dont disposent les services de police. »[98].

L'arrêté ministériel du 28 décembre 2001 portant exécution de certaines dispositions de l'arrêté royal du 30 mars 2001 portant la position juridique du personnel des services de police (ci-après l' « arrêté royal du 30 mars 2001 ») vient préciser les contours et la portée de l'enquête de milieu et des antécédents. La section 3 intitulée « L'enquête de milieu et des antécédents » détaille les personnes qui effectuent l'enquête et précise la liste des bases de données consultées.

En France, dans le cadre d'un recrutement au sein de la police, l'une des conditions requises par le candidat est que celui-ci ne doit pas avoir des *« mentions portées au bulletin n°2 de son casier judiciaire incompatibles avec l'exercice des fonctions »*[99]. En outre une enquête administrative est également effectuée, tel que cela est prévue à l'article L.114-1 du Code de la sécurité intérieure qui dispose en substance que *« Les décisions administratives de recrutement, (…) concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'État, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense (…) peuvent être précédées d'enquêtes administratives destinées à vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées »* et que *« Ces enquêtes peuvent donner lieu à la consultation de traitements automatisés de données à caractère personnel relevant de l'article 31 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification. Les conditions dans lesquelles les personnes intéressées sont informées de cette consultation sont précisées par décret. »*.

D'après l'article 31 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État et qui soit intéressent la sûreté de l'État, la défense ou la sécurité publique, soit ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté, incluant ainsi les traitements opérés par les services de police et de gendarmerie nationales, doivent être autorisés par arrêté du ou des ministres compétents, pris après publication d'un avis motivé de la Commission nationale de l'informatique et des libertés (l'homologue français de la CNPD). Lesdits traitements sont ainsi tous encadrés légalement, comme par exemple le fichier des antécédents judiciaires[100], le fichier d'analyse sérielle[101] ou encore le fichier des personnes recherchées[102].

Par conséquent et contrairement au cadre légal national actuel, respectivement au projet de loi et projet de règlement grand-ducal sous examen, il y a lieu de relever que tant la loi belge que la loi française encadrent de manière

[98] Article 12 de la Loi du 26 avril 2002 relative aux éléments essentiels du statut des membres du personnel des services de police et portant diverses autres dispositions relatives aux services de police.
[99] Article 5 de la Loi n°83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires.
[100] Prévu par les articles 230-6 à 11 du Code de procédure pénale français.
[101] Prévu par les articles 230-12 à 18 du Code de procédure pénale français.
[102] Prévu par l'article 230-19 du Code de procédure pénale français

beaucoup plus précise les traitements de données effectuées dans le cadre de ces procédures de recrutement. Afin de répondre aux exigences de précision et de prévisibilité auxquelles doit répondre un texte légal, la CNPD recommande aux auteurs du projet de loi et du projet de règlement grand-ducal de s'en inspirer.

b. Sur l'accès aux fichiers qui sont légalement accessibles à la Police grand-ducale lors de l'enquête de moralité

La Commission nationale se félicite que l'article 58 de la loi modifiée du 18 juillet 2018 prévoit que la Police grand-ducale *« peut consulter les fichiers qui lui sont légalement accessibles et pour autant que cette consultation est pertinente quant à la finalité recherchée ».*

La CNPD comprend que la Police grand-ducale dispose dès lors d'un accès à l'ensemble des fichiers visés à l'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale. En l'absence de précision quant aux catégories de données contenues dans de tels fichiers et qui seraient effectivement consultées dans le cadre de l'enquête de moralité, la Commission nationale ne peut cependant pas apprécier si de tels accès sont justifiés et proportionnés par rapport à la finalité recherchée, à savoir le recrutement d'un candidat à l'une des fonctions du cadre policier. Ce d'autant plus alors que les accès prévus aux fichiers énumérés à l'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale le sont pour des finalités différentes, à savoir dans l'exercice des missions de police judiciaire et administrative des membres de la Police ayant la qualité d'officier judiciaire ou d'officier de police administrative.

En outre, la CNPD estime que le projet de loi devrait préciser les éventuels accès de la Police grand-ducale à ses propres fichiers, à l'instar des lois belge et française. Ce d'autant plus au vu des inquiétudes récentes des citoyens quant au respect des libertés publiques et la protection de leurs données personnelles dans le domaine policier et judiciaire, il est dès lors important que des clarifications sur les accès aux fichiers et systèmes susmentionnés se retrouvent au niveau de la loi au sens formel.

c. Sur les critères à prendre compte lors de l'appréciation des qualités morales du candidat

La Commission nationale se félicite que les auteurs du projet de loi aient précisé à l'article 1 du projet de loi qui modifie l'article 58 de la loi modifiée du 18 juillet sur la Police grand-ducale quelles seraient les conséquences de l'absence des qualités morales du candidat. En effet, lorsque de telles qualités font défaut, le candidat n'est pas admis au stage.

Cependant, aucune précision quant aux critères pris en compte par la Police grand-ducale lors de l'appréciation des qualités morales du candidat n'apparait dans ledit article ni dans les commentaires des auteurs du projet de loi. Il est cependant nécessaire que les critères pris en compte ou le degré de gravité des antécédents pris en

compte par la Police grand-ducale soient préalablement précisés afin d'en tirer les conséquences, à savoir le refus de l'admission du candidat au stage.

La Commission nationale renvoie pour le surplus à ses développements sous le point I. 2. A. du présent avis.

d. Sur la durée de conservation des données à caractère personnel

Il y a lieu de rappeler qu'en vertu de l'article 5 paragraphe (1) lettre e) du RGPD, les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées.

La Commission nationale regrette que le projet de loi n'indique pas la durée de conservation des données collectées relatives à un candidat et se demande dès lors quels seraient les critères utilisés pour déterminer une telle durée. Des précisions à ce sujet mériteraient d'être apportées par les auteurs du projet de loi.

Dès lors, la CNPD n'est pas en mesure d'apprécier si le principe de durée de conservation limitée des données est respecté.

3. Remarques finales

Enfin, il y a lieu de relever que sur base de la formulation actuelle de l'article 58 de la loi modifiée du 18 juillet 2018, la Commission nationale ne dispose pas de toutes les informations qui lui sont nécessaires afin de lui permettre d'apprécier pleinement si les traitements mis en œuvre dans le cadre de l'enquête de moralité sont conformes au RGPD.

De plus, en l'absence de précisions, certaines questions demeurent en suspens : quelles sont les catégories de données collectées dans le cadre de ces enquêtes de moralité ? Le droit à l'information (articles 13 et 14 du RGPD) des personnes concernées est-il respecté lors de la mise en œuvre des traitements engendrés par l'enquête de moralité ?

Par ailleurs, la Commission nationale constate qu'afin d'accéder à certaines professions il est procédé à des vérifications d'antécédents ou à des enquêtes de moralité ou d'honorabilité ou encore d'enquêtes administratives. De telles enquêtes ou vérifications sont notamment effectuées pour :

- les personnes visées par la procédure de vérifications des antécédents prévue par le Chapitre 3 du projet de règlement grand-ducal relatif à la sûreté de l'aviation civile et aux conditions d'accès à l'aéroport de Luxembourg ;

- les fonctionnaires de l'État et employés de l'État affectés au Service de renseignement de l'État. Une enquête de sécurité est diligentée à leur encontre afin de vérifier notamment s'ils disposent des garanties de moralité[103];
- le candidat à un poste d'employé de l'État qui doit offrir les *« garanties de moralité requises »*[104];
- les candidats à l'examen concours d'attachés de justice. Les candidats pour être admis à l'examen-concours doivent *« présenter les garanties d'honorabilité requises »*[105];
- l'agent qui souhaite exercer l'activité de gardiennage et de surveillance. Celui-ci doit remplir les conditions d'honorabilité nécessaires[106];
- les personnes sollicitant l'octroi d'une autorisation, d'un agrément ou d'un permis en matière d'armes[107].

Bien que cette liste ne soit pas exhaustive, elle permet d'ores et déjà de se rendre compte des disparités qui existent en droit luxembourgeois en ce qui concerne les enquêtes ou vérifications d'antécédents qui seraient diligentées par les administrations ou autorités publiques pour l'accès à certaines professions.

Dans un souci de cohérence, la Commission nationale se demande s'il ne serait pas opportun d'harmoniser l'ensemble de ces procédures en utilisant par exemple des terminologies similaires. En effet, chacune des lois spéciales utilisent une terminologie qui leur est propre alors que certaines notions semblent se recouper. Tel est le cas par exemple avec les notions d'honorabilité et de moralité. L'utilisation d'une terminologie commune permettrait ainsi d'assurer en droit national une cohérence entre ces différentes lois spéciales disparates qui poursuivent pourtant une finalité similaire.

II. Sur le projet de règlement grand-ducal

Le projet de règlement grand-ducal a quant à lui pour objet de préciser les épreuves spéciales organisées par la Police grand-ducale devant être passées pour les candidats désirant accéder aux carrières policières afin de tenir compte des modifications en matière de recrutement au sein de la Police suite à l'alignement les procédures de l'examen-concours pour l'accès aux carrières policières au cadre général de la Fonction publique.

Afin d'avoir une meilleure lecture du texte réglementaire portant sur le recrutement dans les carrières policières, il a été décidé de ne pas modifier le règlement grand-ducal du 17 août 2018 portant : 1° fixation des conditions de recrutement du personnel du cadre policier ; 2° abrogation du règlement grand-ducal du 31 octobre 2001 déterminant les services nationaux et les organismes internationaux dans lesquels le personnel policier peut être employé par ordre du Gouvernement (ci-après le « règlement grand-ducal du 17 août 2018 ») existant, mais de l'abroger et de le remplacer par le projet de règlement grand-ducal sous examen.

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

[103] Cf. articles 21 à 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, telle que modifiée.
[104] Article 3, paragraphe (1), lettre c) de la loi u 25 mars 2015 déterminant le régime et les indemnités des employés de l'État.
[105] Article 2, paragraphe (2), 2) de la loi du 7 juin 2012 sur les attachés de justice.
[106] Article 8, 1) de la loi loi du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance.
[107] Article 14 nouveau du projet de loi n°7425 sur les armes et munitions (document parlementaire n°7425/07).

1. **Sur l'enquête de moralité**

Du fait de l'abrogation du règlement grand-ducal du 17 août 2018, il y a lieu de constater que le présent projet de règlement grand-ducal ne prévoit pas comme condition d'admissibilité à l'épreuve spéciale pour l'admission au stage que le candidat offre les *« garanties de moralité requise au vu de l'enquête de moralité ordonnée par le ministre »,* contrairement à ce qui est précisé dans le règlement grand-ducal du 17 août 2018[108].

Toutefois, la CNPD constate que cette condition a vocation à être maintenue, tel que cela ressort de l'article 1 du projet de loi sous examen. Cette condition étant reprise dans le projet de loi, il n'est dès lors pas nécessaire qu'elle figure également dans le projet de règlement grand-ducal.

2. **Sur l'examen médical**

Il résulte de l'article 23 du projet de règlement grand-ducal sous avis que le candidat avant chaque admission au stage est soumis à un examen médical approfondi, tel que détaillé à l'article 24 dudit projet.

Il y a lieu de rappeler que les données personnelles amenées à être collectées dans le cadre de ces examens sont à qualifier de données sensibles au sens de l'article 9 du RGPD, car celles-ci sont relatives à la santé des candidats. Les traitements de telles données requièrent dès lors une protection spécifique[109] et sont soumis à des exigences plus strictes.

La Commission nationale salue que les auteurs du projet de règlement grand-ducal aient précisé dans le détail les examens médicaux auxquels sont soumis les candidats. De même qu'elle se félicite que les critères d'inaptitude à de tels examens soient précisés à l'annexe A du projet de règlement grand-ducal.

De plus, la CNPD comprend que le médecin de la Division de la santé au travail du secteur public, de l'Administration des services médicaux du secteur public, en charge de tels examens médicaux, transmettra uniquement au service compétent de la Police grand-ducale l'information selon laquelle le candidat est apte ou inapte conformément à l'article 3 du règlement grand-ducal du 5 mars 2004 concernant la santé et la sécurité du travail et le contrôle médical dans la fonction publique, tel que modifié.

3. **Sur l'accès au registre national des personnes physiques**

Le paragraphe (3) de l'article 19 du projet de règlement grand-ducal énumère les pièces qui doivent être produites par le candidat lors de sa demande d'inscription à l'épreuve spéciale.

[108] Voir articles 2 point 3°, 5 point 4° et 15 point 5° du règlement grand-ducal du 17 août 2018 en ce qui concerne les conditions d'admissibilité à l'examen-concours.
[109] Voir les affaires rendues par la CJUE du 8 avril 1992, C-62-90, point 23 et du 5 octobre 1994, C-404/92, point 17.

Le dernier alinéa du paragraphe de l'article précité dispose cependant que ce dernier *« n'a pas besoin de fournir une copie de sa carte d'identité ni un extrait de l'acte de naissance lorsque les données concernant ses nom et prénom(s), sa date de naissance et sa nationalité sont qualifiées d'exactes dans le registre national des personnes physiques et s'il a sa résidence habituelle au Grand-Duché de Luxembourg ».*

La Commission nationale comprend que la Police grand-ducale procède dès lors à la vérification des informations précitées du candidat dans le registre national des personnes physiques.

Or, si l'article 43, 1° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale prévoit l'accès à ce registre aux membres de la Police grand-ducale ayant la qualité d'officier de police judiciaire ou d'officier de police administrative dans le cadre de l'exercice de leurs missions de police judiciaire et de police administrative, il y a lieu de relever que l'accès à de telles données dans le cas présent ne s'effectue pas dans le même cadre mais s'effectue dans le cadre d'un recrutement (voir nos développements au point I. 2. c. du présent avis).

L'accès à ce fichier à des fins de recrutement des candidats aux carrières policières n'est donc pas prévu par l'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale. Il conviendrait dès lors que cette finalité soit prévue par l'article précité.

Ainsi décidé à Esch-sur-Alzette en date du 17 juillet 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

Avis relatif au projet de loi n°7634 modifiant la loi du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 et modifiant: 1° la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2° la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments.

(Délibération n° 18/2020 du 21 juillet 2020)

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 ».*

En date du 20 juillet 2020, Madame la Ministre de la Santé a saisi la Commission nationale à se prononcer sur le projet de loi n° 7634 modifiant la loi du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 et modifiant : 1° la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2° la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments (ci-après le « projet de loi »).

Après analyse du projet de loi, la CNPD constate que les dispositions concernant la protection des droits et libertés des personnes physiques à l'égard du traitement de données à caractère personnel, et plus précisément les articles 5 et 10 dudit projet, n'ont pas changé par rapport aux dispositions correspondantes de la loi actuellement en vigueur du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19.

Néanmoins, la CNPD tient à formuler une remarque concernant le point de départ de la durée de conservation des données à caractère personnel figurant dans le système d'information mis en place par le directeur de la santé afin de suivre l'évolution de la propagation du virus SARS-CoV-2.

Initialement, le projet de loi n°7606 devenu la loi du 24 juin 2020 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre la pandémie Covid-19 prévoyait en son article

9 paragraphe (5) que les données précitées *« sont anonymisées **au plus tard six mois après que la loi cesse de produire ses effets.** »*

Dans son avis n°13/2020 du 8 juin 2020 relatif audit projet de loi n°7606, la CNPD s'était demandée quelles étaient les raisons sanitaires et/ou scientifiques qui ont amené les auteurs du projet de loi à y insérer une durée de conservation spécifique de 6 mois après que la future loi cessera de produire ses effets et elle avait constaté que les législateurs des pays voisins du Luxembourg avaient opté dans ce contexte pour des durées de conservation beaucoup plus courtes.

Suite aux amendements adoptés par la Commission de la Santé et des Sports en date du 11 juin 2020, il a été tenu compte de l'avis de la CNPD et la durée de conservation a été réduite de 6 à 3 mois. Ainsi, l'article 9 paragraphe (5) du projet de loi n°7606 avait la teneur suivante : *« Sans préjudice des dispositions du paragraphe 6 du présent article, leur conservation sous une forme permettant l'identification des personnes est limitée à la durée nécessaire pour prévenir et combattre le Covid-19 et les données sont anonymisées **au plus tard trois mois après que la loi cesse de produire ses effets.** »*

Suite à l'avis complémentaire de la CNPD du 16 juin 2020,[110] des amendements supplémentaires avaient été adoptés par la Commission de la Santé et des Sports.

Sur proposition de l'avis du Conseil d'État du 16 juin 2020, la disposition en question a été modifiée en ce sens que l'article 8 nouveau (article 9 ancien) paragraphe (5) du projet de loi n°7606 prenait la teneur suivante *« les données à caractère personnel traitées **sont anonymisées à l'issue d'une durée de trois mois à compter de la fin de l'état de crise** tel que déclaré par le règlement grand-ducal modifié du 18 mars 2020 portant introduction d'une série de mesures dans le cadre de la lutte contre le Covid-19 et prorogé par la loi du 24 mars 2020 portant prorogation de l'état de crise déclaré par le règlement grand-ducal du 18 mars 2020 portant introduction d'une série de mesures dans le cadre de la lutte contre le Covid-19. »*

A l'instar de la loi abrogée du 24 juin 2020 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre la pandémie Covid-19 et de la loi actuellement en vigueur du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19, le projet de loi sous avis prévoit en son article 10 paragraphe (5) que *« les données à caractère personnel traitées **sont anonymisées à l'issue d'une durée de trois mois à compter de la fin de l'état de crise** tel que déclaré par le règlement grand-ducal modifié du 18 mars 2020 portant introduction d'une série de mesures dans le cadre de la lutte contre le Covid-19 et prorogé par la loi du 24 mars 2020 portant prorogation de l'état de crise déclaré par le règlement grand-ducal du 18 mars 2020 portant introduction d'une série de mesures dans le cadre de la lutte contre le Covid-19. »*

[110] Délibération n°14/2020 du 16 juin 2020.

La CNPD doit avouer que dans son avis n°16/2020 du 8 juillet 2020 concernant le projet de loi n°7622 devenu la loi précitée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19, il lui est échappé de soulever ce point. Or, comme la loi du 24 mars 2020 a prorogé l'état de crise déclaré par le règlement grand-ducal du 18 mars 2020 portant introduction d'une série de mesures dans le cadre de la lutte contre le Covid-19 jusqu'au 24 juin 2020, omettre de modifier ce point aurait comme conséquence que les données à caractère personnel précitées devront être anonymisées pour le 24 septembre 2020, c'est-à-dire trois mois à compter de la fin de l'état de crise. Ceci signifierait que comme l'article 18 du projet de loi sous examen prévoit que la future loi reste applicable jusqu'au 30 septembre 2020 inclus, les données à caractère personnel devraient être anonymisées avant la fin d'applicabilité de la loi. Par ailleurs, plus aucune donnée à caractère personnel ne pourrait être traitée par la direction de la santé à partir du 24 septembre 2020.

La CNPD suppose que cette situation n'ait pas été souhaitée par les auteurs du projet de loi. Ainsi, elle suggère de prévoir comme point de départ, pour ce qui est de la durée après laquelle les données devront être anonymisées, la date de collecte des données ou à tout le moins le jour où la future loi cessera de produire ses effets.

Ainsi décidé à Esch-sur-Alzette en date du 21 juillet 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

ANNEXES

5

Avis relatif au projet de loi n°7524 portant sur la qualité des services pour personnes âgées et portant modification de : 1° la loi modifiée du 16 mai 1975 portant statut de la copropriété des immeubles bâtis ; 2° la loi modifiée du 8 septembre 1998 réglant les relations entre l'État et les organismes œuvrant dans les domaines social, familial et thérapeutique ainsi qu'au projet de règlement grand-ducal portant sur la qualité des services pour personnes âgées.

(Délibération n°19/2020 du 22/07/2020)

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 ».*

Par courrier en date du 6 février 2020, Madame la Ministre de la Famille et de l'Intégration a invité la Commission nationale à se prononcer sur le projet de loi n°7524 portant modification de : 1° la loi modifiée du 16 mai 1975 portant statut de la copropriété des immeubles bâtis ; 2° la loi modifiée du 8 septembre 1998 réglant les relations entre l'État et les organismes œuvrant dans les domaines social, familial et thérapeutique (ci-après le « projet de loi ») ainsi que sur le projet de règlement grand-ducal portant sur la qualité des services pour personnes âgées (« projet de règlement grand-ducal »).

Selon l'exposé des motifs, le présent projet de loi a pour objet de procéder à une refonte du volet concernant les personnes âgées de la loi du 8 septembre 1998 réglant les relations entre l'État et les organismes œuvrant dans les domaines social, familial et thérapeutique (ci-après la « loi ASFT »). Les auteurs du projet de loi précisent encore que le projet de loi a pour objet de *« créer un cadre légal nouveau destiné aux organismes gestionnaires de services et structures pour personnes âgées qui viendra compléter les dispositions relatives à la loi ASFT »*. Le texte sous avis organise ainsi l'action des organismes gestionnaires intervenant dans les domaines du vieillissement actif, du maintien à domicile et du long séjour en structures d'hébergement pour personnes âgées. L'objectif poursuivi par le projet de loi est de préciser la terminologie et de compléter les concepts utilisés par rapport à la réglementation actuelle.

La Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de loi sous examen qui traitent des aspects liés au respect de la vie privée et à la protection des données à caractère personnel. Le présent avis ne traitera pas du projet de règlement grand-ducal car celui-ci ne soulève aucune observation d'un point de vue de la protection des données à caractère personnel et du respect de la vie privée.

I. Sur les traitements de données à caractère personnel effectués par le ministre

1. Sur la création d'un nouveau registre public

Selon l'exposé des motifs, le projet de loi prévoit la création d'un *« registre des structures et services pour personnes âgées qui rendra publique toutes les informations jugées pertinentes à l'attention du grand public, en particulier le projet d'établissement et le contrat type conclu avec les usagers ».*

Ce nouveau registre public est créé sous l'autorité du Ministre ayant dans ses compétences la loi sous avis (ci-après le « ministre ») et contient 7 rubriques intitulées : *« structures d'hébergement pour personnes âgées »*[111], *« services d'aides et de soins à domicile »*[112], *« centres de jour pour personnes âgées »*[113], *« clubs Aktiv Plus »*[114], *« services repas sur roues »*[115], *« services activités seniors »*[116] et *« services téléalarme »*[117]. Le projet de loi énumère pour chacune des rubriques précitées l'ensemble des informations y contenues.

Il y a lieu de constater que ledit registre rendra publique des informations qui ne constituent pas, pour l'essentiel, des données à caractère personnel. Seules les informations relatives au nom du chargé de direction et de ses délégués, le cas échéant, constituent des données à caractère personnel.

La publication de telles données à caractère personnel ne soulève pas de difficulté d'un point de vue de l'application du RGPD alors que cette publication serait effectuée en vertu d'une obligation légale, que constituent les articles 8, 22, 36, 49, 58, 68 et 77 du projet de loi.

2. Sur le traitement de données à caractère personnel effectué par le ministre dans le cadre des demandes d'agrément qui lui sont adressées

La Commission nationale comprend à la lecture du projet de loi que le ministre est amené à collecter et à traiter des données à caractère personnel dans le cadre des demandes d'agrément qui lui sont adressées.

En effet, le projet de loi précise que la demande d'agrément, nécessaire à l'exercice de chacun des services visés par le projet de loi, est adressée par les organismes gestionnaires au ministre, et est accompagnée d'un dossier d'agrément qui comprend un certain nombre de documents et de renseignements[118]. Ces documents et renseignements contiennent des données à caractère personnel.

[111] Article 8 du projet de loi.
[112] Article 22 du projet de loi
[113] Article 36 du projet de loi.
[114] Article 49 du projet de loi.
[115] Article 58 du projet de loi.
[116] Article 68 du projet de loi.
[117] Article 77 du projet de loi.
[118] Cf. article 15 pour les « Services et structures d'hébergement pour personnes âgées » (chapitre 1) ; article 29 pour les « Services d'aides et de soins à domicile » (chapitre 2) ; article 43 pour les « Centres de jour pour personnes âgées » (chapitre 3) ; article 53 pour les « Clubs Aktiv Plus » (chapitre 4) ; article 62 pour les « Services repas sur roues » (chapitre 5) ; article 72 pour les « Services activités seniors » (chapitre 6) ; et article 84 pour les « Services téléalarme » (chapitre 7).

La Commission nationale se demande, dès lors, si le ministre n'est pas amené à tenir un fichier centralisant l'ensemble des données collectées et traitées dans le cadre des demandes d'agrément qui lui sont adressées. Si tel devait être le cas, il convient de rappeler que la tenue d'un fichier de données à caractère personnel collectées et traitées par une autorité administrative doit reposer sur une base légale conformément à l'article 6, paragraphe (3) du RGPD[119].

Cet article 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 définis soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis.

De plus, 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. […] ».*

En vertu des dispositions précitées, ces bases légales devraient établir des dispositions spécifiques visant à déterminer, entre autres, les types de données traitées, les personnes concernées, les entités auxquelles les données peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

La Commission nationale estime donc indispensable, dans l'hypothèse où le ministre tient un fichier, que celui-ci soit prévu par le présent projet de loi. Les dispositions légales portant création d'un tel registre devront contenir les éléments cités au paragraphe ci-dessus.

Par ailleurs, la CNPD entend d'ores et déjà formuler dans les développements ci-après des observations quant au traitement de données à caractère personnel effectué par le ministre dans le cadre des demandes d'agrément qui lui sont adressées.

a. Sur les finalités du traitement

Conformément au principe de la limitation des finalités, les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

[119] L'article 6 paragraphe (3), lu ensemble avec son paragraphe (1) lettres c) et e) , dispose que : « Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par :
a. le droit de l'Union; ou
b. 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 public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. 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. ».

Bien que le projet de loi et le commentaire des articles ne précisent pas expressément les finalités poursuivies par le ministre, la CNPD comprend que les données à caractère personnel collectées et traitées par le ministre le sont aux fins d'octroi et de gestion des agréments. Conformément au principe de la limitation des finalités, lesdites données ne pourraient pas être utilisées par le ministre pour d'autres finalités que celles précitées.

b. <u>Sur les catégories de données à caractère personnel et les personnes concernées</u>

Les organismes gestionnaires, tel que définis aux chapitres 1 à 7 du présent projet de loi, doivent joindre à leur demande d'agrément les documents et renseignements listés par le projet de loi[120].

La CNPD se félicite d'une telle énumération qui précise, pour chaque document ou renseignement visé par le projet de loi, les personnes concernées ainsi que les catégories de données s'y rapportant.

Néanmoins, il ressort des dispositions du projet de loi que le ministre *« peut demander tout autre document ou renseignement indispensable à l'établissement du dossier de la demande d'agrément »*[121]. Les auteurs du projet de loi précisent à ce sujet dans les commentaires des articles que *« Le ministre se réserve le droit de demander tout autre document pour vérifier le bon fonctionnement et la non mise en danger des résidents »*[122] sans toutefois préciser de quels types de documents il pourrait s'agir et les personnes concernées par ces mesures supplémentaires. Si ce *« document ou renseignement indispensable »* contient des données à caractère personnel alors la CNPD estime nécessaire que des précisions à ce sujet soient apportées dans le projet de loi.

En outre, si le ministre devait dans cette hypothèse collecter indirectement des données relatives aux organismes gestionnaires, chargés de direction ou personnel encadrant à partir d'autres fichiers étatiques, alors une telle communication de données entre ministères ou administrations devrait être précisée dans le texte du projet de loi.

c. <u>Sur l'accès aux données</u>

Conformément à l'article 5 paragraphe (1), lettre f) du RGPD les données à caractère personnel doivent être *« traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) »*.

De plus, l'article 32 du RGPD dispose que *« le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »*. Pareilles mesures doivent être mises en œuvre afin d'éviter notamment des accès non-autorisés aux données ou des fuites de données.

[120] Cf. article 15 pour les « Services et structures d'hébergement pour personnes âgées » (chapitre 1) ; article 29 pour les « Services d'aides et de soins à domicile » (chapitre 2) ; article 43 pour les « Centres de jour pour personnes âgées » (chapitre 3) ; article 53 pour les « Clubs Aktiv Plus » (chapitre 4) ; article 62 pour les « Services repas sur roues » (chapitre 5) ; article 72 pour les « Services activités seniors » (chapitre 6) ; et article 84 pour les « Services téléalarme » (chapitre 7).
[121] Paragraphe (3) des articles 15, 29, 43, 53, 62, 72 et 84 du projet de loi.
[122] Les commentaires des articles 29, 43, 53, 62, 72 et 84 renvoient au commentaire de l'article 15.

Parmi ces mesures de sécurité, la Commission nationale estime important que seules les personnes qui en ont besoin dans l'exercice de leurs fonctions et de leurs tâches professionnelles soient habilitées à avoir accès aux données nécessaires. La CNPD recommande dès lors que soit prévu au sein du ministère ayant le projet de loi sous avis dans ses compétences que l'accès à de telles données soit limité aux seuls agents ayant besoin d'en connaître dans le cadre de leur fonction. Il conviendrait également de prévoir les modalités de cet accès et de mettre en place une procédure comportant des garanties appropriées visant à exclure toute utilisation allant au-delà des finalités pour lesquelles ces données sont initialement traitées et notamment, prévoir un système de journalisation (c'est-à-dire un enregistrement dans des « fichiers journaux » ou «logs») des activités des utilisateurs, des anomalies et des événements liés à la sécurité.

d. Sur la durée de conservation des données

Selon l'article 5 paragraphe (1), lettre e) du RGPD, les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées.

La Commission nationale regrette que les auteurs du projet de loi n'aient pas indiqué les durées de conservation des données traitées pour les finalités d'octroi et de gestion des agréments, de sorte qu'elle n'est pas en mesure d'apprécier si en l'occurrence, le principe de durée de conservation limitée des données est respecté concernant la collecte de ces données.

II. Sur les traitements de données à caractère personnel effectués par les organismes gestionnaires

1. Sur le traitement de données à caractère personnel relatif à la condition d'honorabilité professionnelle des chargés de direction et du personnel encadrant

Il convient de relever que les organismes gestionnaires qui sont chargés de la gestion et de l'exploitation des structures ou activités, tels que visés par le projet de loi, ne peuvent employer pour les postes de chargé de direction et de personnel encadrant que les personnes qui répondent aux conditions fixées par le projet de loi pour l'occupation de tels postes.

L'une des conditions qui doit être remplie par le chargé de direction et le personnel encadrant est notamment la condition d' *« honorabilité professionnelle » qui « s'apprécie sur base de ses antécédents pour autant qu'ils concernent des faits ne remontant pas à plus de dix ans »*[123] [124].

Le projet de loi précise encore en ce qui concerne cette condition que : *« constitue un manquement privant le chargé de direction de l'honorabilité professionnelle, tout comportement ou agissement qui affecte si gravement son intégrité professionnelle qu'on ne peut plus tolérer, dans l'intérêt des résidents concernés, qu'il exerce ou continue à*

[123] La même formulation est reprise à l'identique par les articles 4, 18, 33, 47, 57, 66 et 75 du projet de loi en ce qui concerne les chargés de direction.
[124] La même formulation est reprise à l'identique par les articles 5, 19, 34, 48, et 67 du projet de loi en ce qui concerne le personnel encadrant.

exercer la fonction autorisée ou à autoriser »[125] et que : *« constitue un manquement privant l'agent de l'honorabilité professionnelle tout comportement ou agissement qui affecte si gravement son intégrité professionnelle qu'on ne peut plus tolérer, dans l'intérêt des résidents [ou usagers] concernés, qu'il exerce ou continue à exercer la fonction dont il est chargé »*[126].

En l'absence de précisions dans le projet de loi et dans le commentaire des articles, la CNPD se demande quels sont les critères d'appréciation d'une telle honorabilité professionnelle.

Si la condition d'honorabilité professionnelle est appréciée sur base d'antécédents judiciaires, la CNPD comprend que celle-ci se fera conformément aux dispositions légales de l'article 8-5 de la loi du 23 juillet 2016 portant modification 1) de la loi du 29 mars 2013 relative à l'organisation du casier judiciaire, 2) du Code d'instruction criminelle, 3) du Code pénal. Si tel est le cas, elle suggère de préciser dans le texte du projet de loi pour plus de clarté le terme « judiciaires » juste après le terme « antécédents ». Par ailleurs, il serait important de préciser quel degré de gravité des antécédents judiciaires serait pris en compte par les organismes gestionnaires afin d'apprécier la condition d'honorabilité professionnelle du chargé de direction et du personnel encadrant. La CNPD s'interroge notamment si toute inscription au casier judiciaire entraîne automatiquement une appréciation négative en matière d'honorabilité professionnelle ou si, par contre, les inscriptions doivent avoir atteint un certain niveau de gravité.

Si cette condition d'honorabilité professionnelle ne se limite pas aux seuls antécédents judiciaires, la Commission nationale recommande de préciser dans le projet de loi les éléments à prendre en compte pour apprécier l'honorabilité professionnelle.

A titre d'exemple, la CNPD renvoie les auteurs du projet de loi au chapitre 3 intitulé *« L'honorabilité professionnelle »* de la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales et au règlement grand-ducal du 1er décembre 2011 déterminant les modalités de l'instruction administrative prévue à l'article 28 de la loi modifiée du 2 septembre 2011. Ces dispositions légales précisent en effet les éléments sur lesquels l'honorabilité professionnelle s'apprécie.

Enfin, la CNPD comprend que c'est aux organismes gestionnaires d'apprécier la condition d'honorabilité professionnelle du chargé de direction et du personnel encadrant, car ces derniers doivent produire, lors de la demande d'agrément, un certificat attestant que le chargé de direction et le personnel encadrant remplissent cette condition[127]. Toutefois, elle se demande si le ministre n'est pas également susceptible d'apprécier une telle honorabilité sur base des dispositions figurant aux paragraphes (3) des articles 15, 29, 43, 53, 62, 72 et 84 du projet de loi[128]. Si tel était le cas, il conviendrait de le prévoir dans le texte du projet de loi.

Par ailleurs, la Commission nationale se pose la question de la continuité des dispositions de l'article 8 du règlement grand-ducal modifié du 8 décembre 1999 concernant l'agrément à accorder aux gestionnaires de

[125] La même formulation est reprise à l'identique par les articles 4, 18, 33, 47, 57, 66 et 75 du projet de loi.
[126] La même formulation est reprise à l'identique par les articles 5, 19, 34, 48, et 67 du projet de loi.
[127] Cf articles 15, paragraphe (2), 2° et 3°, 29, paragraphe (2), 2° et 3°, 43, paragraphe (2), 2° et 3°, 52, paragraphe (2), 2° et 3°, 62 paragraphe (2), 2°, 72, paragraphe (2), 2° et 3°, 84 paragraphe (2), 2° et 3°.
[128] Cf. nos développements sous le point I, 2, b) du présent avis.

services pour personnes âgées, qui prévoit que la condition d'honorabilité s'apprécie notamment « *sur base de tous les éléments fournis par l'instruction administrative* »? En effet, la CNPD comprend que les dispositions dudit règlement grand-ducal n'auront plus vocation à s'appliquer, dans la mesure où le projet de loi vise à instituer un cadre légal nouveau et à compléter la loi ASFT. Elle se demande toutefois si cette instruction administrative sera toujours effectuée ? Dans l'affirmative, il serait opportun d'inclure également cet élément dans le projet de loi sous examen ainsi que de détailler les données auxquelles peut accéder l'autorité compétente dans le cadre de l'instruction administrative.

2. Sur la création d'un dossier individuel

a. Sur le responsable du traitement

La Commission nationale regrette que le projet de loi ne précise pas quelle entité aura la qualité de responsable du traitement pour les traitements de données à caractère personnel effectués dans le cadre de l'établissement du dossier individuel précité.

Néanmoins, le projet de loi prévoit une obligation pour les organismes gestionnaires en charge de l'exploitation des services et structures d'hébergement pour personnes âgées, services d'aides et de soins à domicile, centres de jour pour personnes âgées, et services téléalarme, d'établir un dossier individuel pour chaque résident ou usager de tels services[129].En effet, il ressort du commentaire des articles des auteurs du projet de loi[130] que l'organisme gestionnaire doit établir pour chaque résident ou usager un dossier individuel.

Le responsable du traitement au sens du RGPD semble donc être l'organisme gestionnaire. La CNPD suggère, dès lors, que soit mentionné dans l'ensemble des articles relatifs au dossier individuel que l'organisme gestionnaire sera le responsable du traitement.

b. Sur la base juridique sur laquelle se fonde le traitement

Il y a lieu de rappeler que tout traitement de données à caractère personnel n'est licite que si au moins une des conditions visées à l'article 6, paragraphe (1), lettres a) à f) est remplie.

Le traitement de données à caractère personnel effectué par les organismes gestionnaires, dans le cadre de la création d'un dossier individuel, se base sur une obligation légale, introduite par le projet de loi aux articles 12, 26, 40 et 81, et ne soulève aucune observation particulière.

Par ailleurs, il y a lieu de relever que les données collectées au titre des articles 12, paragraphe (2), point 7°, 26, paragraphe (2), point 6°, 40, paragraphe (2), point 8° et 81, paragraphe (2), point 7° sont à

[129] Cf article 12 pour les services et structures d'hébergement pour personnes âgées, article 26 pour les services d'aides et de soins à domicile, article 40 pour les centres de jour pour personnes âgées, article 81 pour les services téléalarme.
[130] Cf commentaires des articles 12, 26, 40 et 81.

qualifier de données sensibles au sens de l'article 9 du RGPD, celles-ci étant relatives à la santé des résidents et des usagers.

De tels traitements requièrent une protection spécifique[131] et sont soumis à des exigences plus strictes. Le traitement de données sensibles est, en effet, interdit sauf si l'une des conditions visées au paragraphe (2) de l'article 9 du RGPD est remplie.

En ce qui concerne le traitement des données sensibles visées aux articles précités du projet de loi, la CNPD estime que la condition visée à l'article 9, paragraphe (2), lettre h), du RGPD est remplie dans le cas présent dans la mesure où le dossier individuel est mis en place afin de notamment assurer le suivi médical et la continuité des soins du résident ou de l'usager.

c. <u>Sur les finalités du traitement de données à caractère personnel</u>

Il y a lieu de relever que les articles du projet de loi portant création d'un dossier individuel ne mentionnent pas les finalités du traitement de données à caractère personnel.

Cependant, il ressort du commentaire de l'article 12 que le but du dossier individuel est de faciliter « *la création et le suivi du plan de prise en charge du résident ainsi que l'accès aux données du résident et permet ainsi de retrouver, à tout moment, tous les éléments historiques concernant son parcours et ses activités. Le dossier individuel unique assure la continuité des soins en proposant un dossier commun accessible par les différents intervenants lors de la prise en charge du résident et permet la traçabilité de chaque action sur son dossier en ce qui concerne les aspects médicolégaux.* ». Dès lors, en ce qui concerne l'article 12, la CNPD comprend que les finalités du traitement sont essentiellement le suivi de la prise en charge du résident.

En l'absence de commentaires des auteurs du projet de loi à ce sujet pour les articles 26, 40 et 81, la CNPD se demande si les mêmes finalités sont applicables pour les dossiers individuels visés par les articles précités.

La Commission nationale recommande que les finalités du traitement soient indiquées dans les articles 12, 26, 40 et 81 en tenant compte à chaque fois de la spécificité des services proposés.

d. <u>Sur les catégories de données à caractère personnel</u>

La Commission nationale salue que les catégories de données à caractère personnel collectées par les organismes gestionnaires soient énumérées avec précision dans les articles du projet de loi relatifs au dossier individuel.

[131] Voir les affaires rendues par la CJUE du 8 avril 1992, C-62/90, point 23 et du 5 octobre 1994, C-404/92, point 17.

Toutefois, la Commission nationale part du principe que le numéro d'identification national (matricule) des résidents ou des usagers sera collecté par les organismes gestionnaires lors de l'établissement de tels dossiers individuels.

Si tel est le cas, elle recommande de le préciser dans le texte des articles 12, 26, 40 et 81 du projet de loi pour éviter toutes difficultés futures dans la mesure où l'utilisation du numéro d'identification national est strictement encadrée par la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques[132].

e. Sur l'accès aux données

La Commission nationale salue que le projet de loi énumère les personnes et entités ayant accès aux données à caractère personnel contenues dans le dossier individuel[133]. De même qu'elle se félicite que le projet de loi prévoie que le dossier individuel est accessible aux personnes et entités visées aux paragraphes (1) des articles 12, 26, 40 et 81 pour les informations visées aux paragraphes (2) desdits articles qui les concernent dans l'exercice de leur mission. Il ressort par ailleurs du projet de loi que le ministre n'aura pas accès à de tels dossiers.

En ce qui concerne l'accès à l'Administration d'évaluation et de contrôle de l'assurance dépendance, la CNPD comprend que celle-ci a accès au dossier individuel dans le cadre de ses missions de contrôle telles que détaillées au paragraphe (1) de l'article 384bis.

Enfin, en ce qui concerne l'accès au dossier individuel aux résidents ou aux usagers et, le cas échéant, à leur représentant légal en ce qui concerne leurs données, la Commission nationale se demande si un tel accès n'est pas similaire à celui prévu par l'article 15 du RGPD, qui confère à la personne concernée le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet afin de prendre connaissance du traitement et d'en vérifier la licéité.

Si tel est le cas, il est suggéré que les dispositions légales prévoyant que le résident ou usager, le cas échéant, son représentant légal, puisse accéder à son dossier individuel ou uniquement aux données le concernant pour le représentant légal dans les conditions et conformément à l'article 15 du RGPD.

f. Sur la durée de conservation

Il y a lieu de rappeler qu'en vertu de l'article 5 paragraphe (1) lettre e) du RGPD, les données à caractère personnel ne doivent pas être conservées pus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées.

[132] En effet, l'article 2, paragraphe (6) dispose que « Les actes, documents et fichiers établis pour l'accomplissement d'une prestation de service demandée par la personne dont le numéro est utilisé et pour laquelle une disposition légale ou réglementaire exige la communication du numéro d'identification doivent contenir ce numéro ».

[133] cf. paragraphe 1 des articles 12, 26, 40 et 81 du projet de loi.

Le projet de loi prévoit pour chacun des dossiers individuels une durée de conservation de 10 ans à compter de la fin du contrat d'hébergement[134], du contrat de prise en charge[135] ou du contrat de services[136].

La CNPD part de l'hypothèse que pour la fixation de la durée de conservation de 10 ans, les auteurs du projet de loi aient voulu s'aligner sur la durée de conservation des dossiers médicaux des patients prévue à l'article 15 (4) de la loi du 24 juillet 2014 relative aux droits et obligations du patient. Or, en l'absence d'explications des auteurs du projet de loi dans le commentaire des articles précités quant à la nécessité de conserver les données pendant une durée de 10 ans, la CNPD n'est pas en mesure d'apprécier si cette durée est adéquate et proportionnée aux finalités poursuivies.

g. Sur la sécurité du traitement

Il y a lieu de 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.

Il convient plus particulièrement d'attirer l'attention des auteurs du projet de loi sur le fait que dans la mesure où des données sensibles (données de santé) sont amenés à être traitées, les organismes gestionnaires devront mettre en place des mesures de protection afin d'assurer la confidentialité et la sécurité de telles données, dont notamment un système de journalisation (c'est-à-dire un enregistrement dans des « fichiers journaux » ou «logs») des activités des utilisateurs, des anomalies et des événements liés à la sécurité. En effet, la divulgation de données sensibles pourrait causer un préjudice grave aux usagers ou aux résidents.

Ainsi décidé à Esch-sur-Alzette en date du 22 juillet 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

[134] Dernier alinéa du paragraphe (2) de l'article 12.
[135] Dernier alinéa du paragraphe (2) de l'article 26 et paragraphe (3) de l'article 40.
[136] Paragraphe (3) de l'article 81.

ANNEXES

5

Avis relatif à la proposition de loi n°7257 portant modification de la loi modifiée du 21 septembre 2006 sur le bail à usage d'habitation et modifiant certaines dispositions du Code civil.

(Délibération n° 20/2020 du 28/07/2020)

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 ».*

Par courrier en date du 7 mai 2020, Monsieur le Ministre du Logement a invité la Commission nationale à se prononcer sur la proposition de loi n°7257 portant modification de la loi modifiée du 21 septembre 2006 sur le bail à usage d'habitation et modifiant certaines dispositions du Code civil (ci-après la « proposition de loi »).

La présente proposition de loi a pour objet de modifier la loi du 21 septembre 2006 sur le bail à usage d'habitation et modifiant certaines dispositions du code civil (ci-après la « loi du 21 septembre 2006 »). Les mesures prévues par la proposition de loi ont pour objet de faire face à la crise du logement que connaît actuellement le Grand-Duché de Luxembourg.

Les principaux points de la proposition de loi sont les suivants :

- l'introduction d'un coefficient de pondération (« valeur de référence du loyer ») destiné à limiter l'incidence des prix d'achat des immeubles de location sur les loyers légalement possibles ;
- l'obligation pour les bailleurs d'inscrire dans tout nouveau contrat de bail le capital investi ainsi que la valeur de référence du loyer ;
- la redéfinition de la notion de « logement de luxe » figurant dans la loi précitée du 21 septembre 2006 ; et
- la création de la commission nationale des loyers avec des compétences nationales, notamment pour la collecte de données relatives aux baux d'habitation et pour la fixation subséquente de la « valeur de référence du loyer ».

Le présent avis limitera ses observations à l'article 1 point 5° de la proposition de loi en ce qu'il crée une banque de données qui sera tenue par la commission nationale des loyers, seul article ayant trait à la protection des données à caractère personnel.

1. Remarques liminaires

L'article 1 point 5° de la proposition de loi introduit un nouveau paragraphe (6) à l'article 3 de la loi du 21 septembre 2006 qui prévoit l'obligation pour chaque bailleur d'inscrire dans tout nouveau contrat de bail le capital investi ainsi que la valeur de référence du loyer. Le bailleur ou son représentant devra, en outre, transmettre une copie du contrat de bail à la commission nationale des loyers qui enregistrera dans une banque de données *« soumise 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 »*[137] *« la localisation du logement, le type de logement, les nom, prénom et adresse du propriétaire, les nom et prénom du locataire, le capital investi, celui ajusté à l'année de référence 1995, le montant réévalué et décoté, la valeur de référence du loyer et le montant du loyer »*. Les nom, prénom et adresse du propriétaire, et les nom et prénom du locataire constituent des données à caractère personnel au sens de l'article 4, paragraphe (1) du RGPD.

La Commission nationale se félicite que la proposition de loi prévoit le principe de la création d'une telle banque de données conformément à l'article 6, paragraphe (3) du RGPD[138]. Cet article prévoit, en effet, 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.

Toutefois et bien que le principe de la création d'une telle banque de données soit prévue dans la proposition de loi, la Commission nationale relève que certains éléments relatifs au traitement de données ne sont pas (ou pas suffisamment) précisés dans la proposition de loi.

En effet, 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. […] »*. En vertu des dispositions précitées, ces bases légales devraient contenir des dispositions spécifiques concernant, entre autres, les types de données traitées, les personnes concernées, les

[137] La Commission nationale tient à rappeler que la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel a été abrogée par l'article 72 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. Il convient dès lors de se référer à la législation actuellement en vigueur.

[138] L'article 6, paragraphe (3) dispose 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 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 »*.

entités auxquelles les données peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

2. <u>Sur la détermination des finalités du traitement</u>

Il y a lieu de relever que conformément à l'article 5 paragraphe (1), lettre 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 (…) ».*

Tel qu'exposé ci-avant, l'article 6 paragraphe (3) du RGPD, lu ensemble avec son paragraphe (1) lettre 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.

Le considérant (41) du RGPD précise 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 et de la Cour européenne des droits de l'homme. ».*

Or, il y a lieu de constater que la rédaction actuelle de la proposition de loi ne respecte pas les dispositions précitées alors que les finalités des traitements visés par le nouvel article 3 paragraphe (6) de la loi du 21 septembre 2006 ne résultent pas clairement de la proposition de loi.

Des précisions quant aux finalités qui seraient poursuivies ne sont également pas apportées par les auteurs de la proposition de loi. En effet, ces derniers se limitent à exposer, dans leur commentaire de l'article 1 point 5° de la proposition de loi, le procédé selon lequel les données seront collectées par la commission nationale des loyers.

Ainsi, il est précisé qu' : *« une copie de chaque contrat de bail conclu ou modifié après l'entrée en vigueur de la présente loi, est transmise endéans un mois suivant la conclusion par le bailleur ou son représentant — par exemple un agent immobilier — à la commission nationale des loyers », puis « la commission nationale enregistre la localisation du logement, le type de logement, les nom, prénom et adresse du propriétaire, les nom et prénom du locataire, le capital investi, celui ajusté à l'année de référence 1995, le montant réévalué et décoté, la valeur de référence du loyer et le montant du loyer convenu dans une banque de données ». Il est encore spécifié que « (…) la commission nationale vérifie les copies de contrats de baux qui leur ont été transmises en vertu de ces dispositions. Au cas où la commission nationale constate qu'un contrat ne répond pas aux prescriptions de la présente loi, elle prend l'initiative pour faire redresser les modalités contractuelles en question ».*

La CNPD comprend dès lors que les données à caractère personnel collectées par la commission nationale des loyers via la copie du contrat de bail le seraient pour deux finalités distinctes, l'une serait afin de répondre à sa mission de contrôle et la deuxième serait afin que ces données figurent dans la banque de données précitée.

Il y a encore lieu de relever que d'après l'exposé des motifs la banque de données précitée permet de mettre *« les données statistiques, anonymisées, à disposition de l'Observatoire de l'Habitat, du STATEC et autres centres de recherche et de statistique, afin d'améliorer le monitoring du marché de la location »*[139].

Néanmoins, comme relevé par le Conseil d'État dans son avis du 28 avril 2020 relatif à la présente proposition de loi : *« La communication des données personnelles pourrait encore se comprendre, dans une certaine mesure, dans l'optique où la commission nationale des loyers serait en charge de la fixation des coefficients de pondération. Or, d'après les auteurs de la proposition de loi, cette fixation appartiendra à l'Institut national de la statistique et des études économiques. »*[140].

Dès lors, à l'instar du Conseil d'État, la CNPD estime nécessaire que les finalités des traitements mis en œuvre par la commission nationale des loyers soient clairement spécifiées dans le texte de la proposition de loi et estime donc indispensable que les auteurs de la proposition de loi indiquent précisément quelles catégories de données sont traitées pour quelles finalités.

Cette problématique se pose avec d'autant plus d'importance que, comme le souligne le Conseil d'État, la proposition de loi *« prévoit de surcroît des sanctions pénales conséquentes en cas de manquement à l'obligation de communication ».*

En l'absence de précision des finalités poursuivies, la Commission nationale se demande comment la commission nationale des loyers dans le cadre de la mise en œuvre des traitements de données à caractère personnel visés par la présente proposition de loi est en mesure de déterminer si elle respecte les principes de minimisation des données et de limitation de la conservation des données alors que conformément au paragraphe (2) de l'article 5 du RGPD le responsable du traitement *« est responsable du respect du paragraphe (1)*[141] *et est en mesure de démontrer que celui-ci est respecté »* (cf. sections 3 et 5 du présent avis).

La CNPD ne peut d'ailleurs qu'approuver les propos du Conseil d'État en ce qu'il *« ne saurait admettre qu'à défaut de détermination claire d'une finalité spécifique du traitement, les données puissent être conservées et utilisées par la commission nationale des loyers au-delà de l'examen immédiat auquel elle peut procéder au titre de l'article 5 de la proposition de loi sous avis. »*[142].

[139] Page 27 de la proposition de loi.
[140] Document parlementaire n°7257/05, page 4.
[141] L'article 5 paragraphe (1) du RGPD dispose que : *« (1) Les données à caractère personnel doivent être : (…)*
c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données); (…)
e) 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; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation); (…) »
[142] Document parlementaire n°7257/05, page 4.

3. Sur le principe de minimisation des données à caractère personnel

L'article 5 paragraphe (1), lettre 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 »*.

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 à la commission nationale des loyers dans le cadre du traitement mis en œuvre.

Or, en l'absence de précision quant aux finalités qui seraient poursuivies par la commission nationale des loyers dans le cadre de la mise en œuvre des traitements de données à caractère personnel visés par l'article 1 point 5° de la proposition de loi, la CNPD n'est pas en mesure d'apprécier si les catégories de données énumérées à l'article précité sont bien adéquates, pertinentes et limitées à ce qui est nécessaire aux regard de ces finalités. Par conséquent, la CNPD ignore si le principe de minimisation des données serait en l'espèce respecté.

La Commission nationale tient, en outre, à souligner l'importance de ce principe alors 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 sans la jurisprudence de la Cour européenne des droit de l'Homme[143].

Bien qu'il ne lui soit pas possible d'apprécier si le principe de minimisation serait respecté, la CNPD se félicite que le point 5° de l'article 1 de la proposition de loi énumère les données à caractère personnel amenées à figurer dans la banque de données[144]. Toutefois, elle constate qu'il ne ressort pas clairement de la proposition de loi si les copies de contrat de bail - qui contiendront indéniablement encore d'autres données personnelles que celles énumérées à l'article 1 point 5° - sont également amenées à figurer dans la banque de données alors que les bailleurs ou leur représentant ont l'obligation de fournir une telle copie à la commission nationale des loyers, ou si de telles copies figureront dans une banque de données distincte alors que l'exposé des motifs précise que la commission nationale *« centralisera les contrats de baux »*.

Des précisions à ce sujet mériteraient d'être apportées par les auteurs de la proposition de loi.

4. Sur la consultation des données figurant dans la banque de données tenue par la commission nationale des loyers

La proposition de loi prévoit que *« La banque des données enregistrées par la commission nationale des loyers peut être consultée pour des besoins statistiques et de recherche. Les modalités de consultation sont fixées par règlement grand-ducal »*.

[143] Voir notamment CEDH, affaire Libert c. France, 22 février 2018, paragraphe 43.

[144] Selon l'article 1 point 5° de la proposition de loi, la commission nationale des loyers serait amenée à collecter *« la localisation du logement, le type de logement, les nom, prénom et adresse du propriétaire, les nom et prénom du locataire, le capital investi, celui ajusté à l'année de référence 1995, le montant réévalué et décoté, la valeur de référence du loyer et le montant du loyer »* ainsi que la *« (…) copie de chaque contrat de bail conclu ou modifié après l'entrée en vigueur de la présente loi (…) »*.

Les auteurs de la proposition de loi précisent dans le commentaire des articles que *« La banque des données enregistrées par la commission nationale des loyers peut être consultée pour des besoins statistiques et de recherche, comme par exemple le STATEC, l'Observatoire de l'Habitat, des centres de recherche. A cette fin les données sont évidemment rendues anonymes. Les modalités de consultation sont fixées par règlement grand-ducal ».*

En l'absence d'un projet de règlement grand-ducal fixant les modalités de consultation de la banque de données, la Commission nationale n'est pas en mesure d'apprécier pleinement si la consultation des données contenues dans la *« banque de données enregistrées par la commission nationale des loyers »* est conforme au RGPD.

Cependant, elle souhaite d'ores et déjà relever qu'il ressort du commentaire des auteurs de la proposition de loi quant aux dispositions énoncées ci-avant, que seules des données rendues anonymes seraient communiquées au STATEC et à l'Observatoire de l'Habitat et à des *« centres de recherche »*. La CNPD comprend dès lors que le STATEC, l'Observatoire de l'Habitat et les « centres de recherche » (dont l'identité devrait le cas échéant être précisée) n'auraient, en réalité, pas accès à ladite banque de données mais seulement accès à des données anonymisées par la commission nationale des loyers.

Dans la mesure où les commentaires des auteurs de la proposition de loi diffèrent des dispositions légales de l'article 1 point 5° de la proposition de loi, il y a lieu de mentionner clairement dans la proposition de loi s'il s'agit d'un accès direct aux données à caractère personnel figurant dans la banque de données ou s'il s'agit d'une communication de données anonymisées, obtenues sur base des données figurant dans la banque de données.

Par ailleurs, l'article 1 point 5° de la proposition de loi visant une consultation de données *« pour des besoins statistiques et de recherche »,* il convient de rappeler qu'en vertu du principe de limitation des finalités (article 5 du RGPD), les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Ainsi, les données ne doivent pas être traitées pour des finalités « incompatibles » avec les finalités d'origine. Néanmoins, le considérant 50 du RGPD précise que « Le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques devrait être considéré comme une opération de traitement licite compatible ».

Les articles 6 paragraphe (4) et 89 du RGPD ainsi que l'article 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, précisent les mesures appropriées qui doivent être mises en œuvre par le responsable du traitement lors de tels traitements ultérieurs de données.

La commission nationale des loyers devra dès lors remplir l'ensemble des conditions prévues par les dispositions légales énoncées ci-dessus afin de permettre la communication des données à caractère personnel contenues dans ladite banque de données au STATEC, à l'Observatoire de l'Habitat et à des *« centres de recherche »*.

Comme pré-mentionné, le texte même de la proposition de loi ne précise pas que les données devront être anonymisées pour *« des fins statistiques et de recherche »*, mais seul le commentaire des articles y fait référence. Ceci dit, la CNPD relève qu'une telle mesure constitue en effet une des mesures appropriée visée par l'article 65 de la loi du 1er août 2018 précitée. Cet article dispose en effet que : *« l'anonymisation, la pseudonymisation au sens de l'article 4, paragraphe 5, du règlement (UE) 2016/679 ou d'autres mesures de séparation fonctionnelle garantissant que les données collectées à des fins de recherche scientifique ou historique, ou à des fins statistiques, ne puissent être utilisées pour prendre des décisions ou des actions à l'égard des personnes concernées »*.

Cependant, la Commission nationale entend attirer l'attention des auteurs de la proposition de loi sur le fait que l'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible. Au contraire, la pseudonymisation, telle que définie par l'article 4 paragraphe (5) du RGPD, est un traitement de données personnelles réalisé de *« telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »*.

Par conséquent, il est important que les auteurs de la proposition de loi analysent si la commission nationale des loyers communiquera des données pseudonymisées au sens du RGPD, ou des données véritablement anonymisées ou « rendues anonymes », auquel cas le RGPD n'aurait pas vocation à s'appliquer à partir du moment où de telles données ne permettent plus aucune identification de la personne par quelque moyen que ce soit et ce de manière irréversible.

Enfin, la Commission nationale suggère également que les auteurs de la proposition de loi reprennent la terminologie exacte du RGPD et 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, en ce qui concerne les traitements de données à caractère personnel *« à des fins statistiques »* ou à des fins *« de recherches scientifique ou historique »* et non pas comme mentionné dans la présente proposition de loi *« à des fins statistiques et de recherche »*.

5. <u>Sur la durée de conservation des données à caractère personnel</u>

Conformément à l'article 5 paragraphe (1), lettre e) du RGPD, les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées.

En l'absence de précision d'une durée de conservation dans la proposition de loi ou dans le commentaire des articles, la CNPD n'est pas en mesure d'apprécier si en l'occurrence, le principe de durée de conservation limitée des données est respecté concernant la collecte des données à caractère personnel consignées dans la banque de données visée par la présente proposition de loi ainsi que concernant les copies de contrat de bail.

La CNPD estime dès lors nécessaire que les auteurs de la proposition de loi précisent dans le texte de l'article 1 point 5° quelle est la durée de conservation ou *a minima* les critères permettant de déterminer quelle est la durée de conservation proportionnée pour les catégories de données énoncées ci-avant.

Ainsi décidé à Belvaux en date du 28 juillet 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

ANNEXES

5

Avis relatif au projet de loi n°7645 modifiant la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 et modifiant: 1° la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2° la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments.

(Délibération n°22/2020 du 10 septembre 2020)

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 ».*

En date du 3 septembre 2020, Madame la Ministre de la Santé a saisi la Commission nationale à se prononcer sur une série d'amendements gouvernementaux relative au projet de loi n°7645 modifiant la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 et modifiant : 1° la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2° la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments (ci-après le « projet de loi »). Lesdits amendements ont été approuvés par le Conseil de gouvernement dans sa séance du 28 août 2020 et par vidéoconférence en date du 2 septembre 2020.

Dans un courrier du 5 août 2020 à l'attention de Madame la Ministre de la Santé,[145] la CNPD avait fait suite à la demande d'avis initial concernant précisément le projet de loi n°7645. Dans ledit courrier, la CNPD avait constaté que les auteurs dudit projet de loi avaient suivi son argumentation[146] en ce qui concerne le point de départ de la durée après laquelle les données à caractère personnel figurant dans le système d'information mis en place par le directeur de la santé afin de suivre l'évolution de la propagation du virus SARS-CoV-2 devraient être anonymisées. En effet, l'article 10 paragraphe (5) de la version initiale du projet de loi prévoyait que les données à caractère personnel traitées sont anonymisées au plus tard à l'issue d'une durée de trois mois après que la loi aura cessé de produire ses effets. Pour cette raison, la CNPD n'avait pas estimé nécessaire d'aviser à ce moment-là le projet de loi sous objet.

[145] Ledit courrier a été publié sur le site internet de la Chambre des députés, disponible sous le lien suivant : https://chd.lu/wps/PA_RoleDesAffaires/FTSByteServingServletImpl?path=87A9599EDE62F169AA77DC4B5C45C83FF023D14EBB8E9616EA6C696E2FE1ACB1E9929DE543B86AC5030E1A177B55996B$6B72A85BA47BBAC5380CCB9F515EA5D0.

[146] Comme précisé dans l'avis n°18/2020 de la CNPD du 21 juillet 2020 relatif au projet de loi n°7634 devenu la loi abrogée du 24 juin 2020 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre la pandémie Covid-19.

Par l'amendement gouvernemental n°6, Madame la Ministre de la Santé propose d'amender le libellé du nouvel article 6 (ancien article 2) du projet de loi n°7645 en ce sens que l'article 10 paragraphe (5) de la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 prévoit dorénavant que les données à caractère personnel en cause ne sont plus anonymisées, mais pseudonymisées, et ceci dans un délai de trois mois après leur collecte.

En ce qui concerne tout d'abord la fixation du point de départ de la durée après laquelle les données à caractère personnel devront être pseudonymisées, la CNPD ne peut, dans un but de proportionnalité et de nécessité, que soutenir le choix de prendre la date de collecte des données et non plus le jour où la future loi cessera de produire ses effets, surtout si on prend en compte la volonté du gouvernement de prolonger l'applicabilité de la loi précitée du 17 juillet 2020 au 31 décembre 2020 inclus[147]. Or, la Commission nationale ne peut pas approuver la décision d'insérer dans le projet de loi sous examen uniquement une obligation pour la direction de la santé de pseudonymiser et non pas d'anonymiser, voire de supprimer les données collectées après un certain délai. Le commentaire de l'amendement n°6 ne précise d'ailleurs pas pourquoi le terme « anonymisées » a été remplacé par le terme « pseudonymisées ».

La Commission nationale tient à préciser dans ce contexte qu'elle salue la mise en place d'une procédure de pseudonymisation des données traitées par la direction de la santé, une telle procédure étant à considérer comme une des mesures techniques et organisationnelles que le responsable du traitement peut être amené à mettre en place, afin d'atténuer les risques pour les personnes concernées.[148] Or, il est essentiel de savoir que les données à caractère personnel qui ont fait l'objet d'une pseudonymisation peuvent par définition toujours être attribuées à une personne physique déterminée par le recours à des informations supplémentaires.[149] Ainsi, la CNPD ne peut pas être d'accord avec l'affirmation des auteurs des amendements dans le commentaire de l'amendement n°6 du projet de loi qu'il *« convient encore de retenir le procédé de la pseudonymisation qui empêche que les données à caractère personnel soient reliées à l'identité originale d'une personne physique ».*

Par conséquent, comme les données pseudonymisées sont toujours à considérer comme des informations concernant une personne physique indirectement identifiable, le RGPD s'applique intégralement à leur traitement. Ce n'est que si les données à caractère personnel sont rendues totalement anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable, par quelque moyen que ce soit, que le RGPD ne s'applique plus.[150] Or, comme ceci n'est pas le cas en l'état actuel du texte du projet de loi, il se pose un certain nombre de questions relatives au traitement des données pseudonymisées, comme par exemple : qui gère la pseudonymisation ? A-t-on recours à un sous-traitant ? Comment la pseudonymisation est-elle effectuée d'un point de vue technique ? Qui peut faire une ré-identification et qui contrôle, le cas échéant, la légitimité de ces ré-identifications ? Si les données sont pseudonymisées pour faire un suivi sur du long terme, quelles sont les finalités poursuivies ? Est-ce que les données sont pseudonymisées à des fins de recherches scientifiques ou statistiques ou la pseudonymisation des données constitue-t-elle une mesure de sécurité technique et organisationnelle ou

[147] Comme prévu par l'amendement n°7 du projet de loi.

[148] Comme prévu par l'article 32 paragraphe (1) lettre a) du RGPD, à voir aussi l'article 25 (1) du RGPD qui dispose que : *« […] le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données […]. »*

[149] L'article 4 point (5) du RGPD définit la pseudonymisation comme *« traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable. »*

[150] Voir le considérant (26) du RGPD.

poursuit-on ces deux finalités ? Les données pseudonymisées sont-elles mises à la disposition de tiers à des fins de recherches scientifiques ?

Par ailleurs, comme le RGPD s'applique intégralement aux données pseudonymisées, les auteurs du projet de loi n°7645 doivent impérativement prendre en compte l'article 5 paragraphe (1) lettre (e) du RGPD prévoyant que les données à caractère personnel peuvent 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 »*. Il ressort par ailleurs du considérant (45) du RGPD que lorsque 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, il devrait appartenir au droit de l'Union ou au droit d'un État membre d'établir, entre autres, la durée de conservation des données. De plus, l'article 5 paragraphe (1) lettre (b) du RGPD prévoit que 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 »*.

Ainsi, comme déjà mentionné dans son avis 13/2020 du 8 juin 2020 relatif au projet de loi n°7606, la CNPD rappelle que *« la durée de conservation doit être déterminée en fonction de l'objectif ayant conduit à la collecte des données en cause. Une fois cet objectif atteint, ces données devraient être supprimées ou anonymisées (afin notamment de produire des statistiques). »*

Par ailleurs, comme susmentionné et en tenant compte du fait que la législation réglementant les mesures de lutte contre la pandémie Covid-19 sera, le cas échéant, prolongée tant que le législateur l'estime nécessaire, la Commission nationale favorise dorénavant comme point de départ de la durée après laquelle les données à caractère personnel devront être pseudonymisées la date de collecte des données et non pas le jour où la future loi cessera de produire ses effets. Elle s'aligne dans ce contexte à l'avis de la Commission consultative des Droits de l'Homme du 28 août 2020 concernant le projet de loi sous examen qui estime de même que *« dans un but de proportionnalité et de nécessité, une telle approche, plus stricte, serait à privilégier. »*

Pour conclure, au regard du RGPD il est ainsi nécessaire et primordial de définir dans le corps du texte du projet de loi une durée de conservation des données à caractère personnel conservées sous forme pseudonymisée au sein du système d'information de la direction de la santé qui soit proportionnée au regard de la finalité poursuivie, c'est-à-dire que le projet de loi devrait préciser un délai au bout duquel les données pseudonymisées ou non devraient être supprimées définitivement ou totalement anonymisées au sens du RGPD. En l'absence d'une telle disposition, il y a lieu de conclure que les données pseudonymisées peuvent être conservées sans limitation dans le temps, ce qui serait incompatible avec les règles du RGPD.

Ainsi décidé à Belvaux en séance plénière et adopté à distance à l'unanimité des quatre Commissaires en date du 10 septembre 2020.

Pour la Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Avis relatif aux amendements gouvernementaux au projet de loi n°7683 modifiant 1) la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 et modifiant : 1° la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2° la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments ; 2) la loi du 23 septembre 2020 portant des mesures concernant la tenue de réunions dans les sociétés et dans les autres personnes morales.

(Délibération n°23/2020 du 27 octobre 2020)

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 ».*

En date du 26 octobre 2020, Madame la Ministre de la Santé a saisi la Commission nationale à se prononcer sur les amendements gouvernementaux au projet de loi n°7683 modifiant 1) la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 et modifiant : 1° la loi modifiée du 25 novembre 1975 concernant la délivrance au public des médicaments ; 2° la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments ; 2) la loi du 23 septembre 2020 portant des mesures concernant la tenue de réunions dans les sociétés et dans les autres personnes morales (ci-après : « le projet de loi n°7683 »). Lesdits amendements gouvernementaux au projet de loi n°7683 ont été approuvés par le Conseil de gouvernement dans sa séance du 26 octobre 2020.

L'amendement 5 du projet de loi n°7683 vise à modifier le nouvel article 6 (ancien article 5) en ce sens que les personnes infectées doivent donner des renseignements sur leur état de santé et sur l'identité des personnes avec lesquelles elles ont eu des contacts susceptibles de générer un haut risque d'infection, au directeur de la santé ou son délégué, aux fonctionnaires et employés désignés à cet effet par le directeur de la santé, et dorénavant aussi aux salariés mis à disposition du ministère de la santé en application de l'article L. 132-1 du Code du travail relatif au prêt temporaire de main-d'œuvre.

Il ressort du commentaire de l'amendement 5 précité du projet de loi n°7683 qu'il a pour objet *« de pouvoir recourir en sus des fonctionnaires et employés, à des salariés mis à la disposition du ministère de la santé dans le cadre d'un prêt de main d'œuvre en application des dispositions du Code du travail y afférentes, et ce afin de recueillir les informations sur l'état de santé des personnes infectées et sur l'identité des personnes avec lesquelles elles ont été en contact. »*

La CNPD comprend absolument qu'en raison de l'augmentation vigoureuse des nouvelles infections ces derniers jours et corrélativement de la charge de travail de l'équipe du traçage de contacts de la direction de la santé, il est nécessaire d'augmenter en parallèle le nombre de collaborateurs de ladite équipe. Néanmoins, elle constate que l'article 10 paragraphe (3) du projet de loi n°7683, prévoyant qui est autorisé dans le cadre du traçage des contacts d'accéder aux données des personnes infectées ou à haut risque d'être infectées contenues dans le système d'information mis en place à cet effet, n'a pas été modifié afin d'ajouter les salariés précités.

Ainsi, la CNPD recommande aux auteurs du projet de loi n°7683 d'insérer dans l'article 10 paragraphe (3) dudit projet après « Seuls les médecins et professionnels de la santé ainsi que les fonctionnaires et employés » les mots « et les salariés mis à disposition du ministère de la santé en application de l'article L. 132-1 du Code du travail ». L'article 10 paragraphe (3) du projet de loi n°7683 aurait alors la teneur suivante :

« Seuls les médecins et professionnels de la santé ainsi que les fonctionnaires et employés ***et les salariés mis à disposition du ministère de la santé en application de l'article L. 132-1 du Code du travail****, nommément désignés par le directeur de la santé, sont autorisés à accéder aux données relatives à la santé des personnes infectées ou à haut risque d'être infectées. Ils accèdent aux données relatives à la santé dans la stricte mesure où l'accès est nécessaire à l'exécution des missions légales ou conventionnelles qui leur sont confiées pour prévenir et combattre la pandémie de Covid-19 et sont astreints au secret professionnel dans les conditions et sous les peines prévues à l'article 458 du Code pénal. »*

Cet ajout aurait par ailleurs comme conséquence que lesdits salariés seraient aussi soumis dans ce contexte aux sanctions pénales prévues à l'article 458 du code pénal en cas de nonrespect du secret professionnel. Sous ces conditions restrictives, la CNPD estime que les accès supplémentaires au système d'information apparaissent légitimes.

Ainsi décidé à Esch-sur-Alzette en date du 27 octobre 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

Avis relatif au projet de loi n°7635 portant introduction d'une série de mesures temporaires en matière de sécurité et santé au travail dans le cadre de la lutte contre le COVID-19.

(Délibération n°24/2020 du 30 octobre 2020)

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.

A ce titre, la Commission nationale s'autosaisit pour aviser le projet de loi n°7635 portant introduction d'une série de mesures temporaires en matière de sécurité et santé au travail dans le cadre de la lutte contre le COVID-19 (ci-après le « projet de loi ») et plus précisément son article 2 paragraphe (2).

L'auto-saisine de la CNPD intervient dans le cadre de nombreuses demandes d'information et de réclamations introduites auprès d'elle concernant d'une part les données, notamment de santé, que les salariés seraient autorisés à communiquer à l'employeur en cas de suspicion ou de contamination au virus SARS-CoV-2, et d'autres part les obligations de l'employeur quant au traitement de ces données.

L'article 2 paragraphe (2) du projet de loi sous avis, prévoit que *« les salariés doivent signaler immédiatement, à l'employeur ou aux salariés désignés et aux délégués à la sécurité et à la santé, toute situation de travail dont ils ont un motif raisonnable de penser qu'elle présente un danger grave et immédiat pour la sécurité et la santé dans le cadre de l'épidémie de COVID-19 ».*

Or, la Commission nationale se demande ce que recouvrent les *« situation[s] de travail dont [les salariés] ont un motif raisonnable de penser qu'elle[s] présente[nt] un danger grave et immédiat pour la sécurité et la santé dans le cadre de l'épidémie de COVID-19 »,* et s'interroge sur les données de santé qui pourraient être transmises à l'occasion de ces signalements. Est-ce qu'un salarié devrait communiquer à son employeur les symptômes qu'il présente, le fait qu'il ait été récemment en contact avec une personne infectée, ou le résultat positif d'un test diagnostique de l'infection au virus SARS-CoV-2? L'employeur pourrait-il exiger la communication de telles

informations ou la production du résultat d'un test positif ou négatif réalisé par un salarié ? Ou bien est-ce que la transmission par le salarié d'un avis d'aptitude ou d'inaptitude à reprendre le travail émis par un professionnel de santé est estimé suffisant, à l'instar d'autres arrêts de maladie, conformément aux obligations en matière de droit du travail ?

Dans l'hypothèse où il faudrait interpréter cette disposition en ce sens que des données de santé devraient être transmises par les salariés aux employeurs (résultat d'un test diagnostique, signalisation de symptômes, et/ou signalisation de contacts avec un personne infectée), la Commission nationale se demande encore quels traitements les employeurs pourraient alors mettre en œuvre concernant ces catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD, dites « données sensibles », et selon quelles modalités ?

La CNPD tient à rappeler qu'en vertu de l'article 9 du RGPD, il est en principe interdit de traiter des données dites « sensibles », sauf si l'une des exceptions prévues au paragraphe (2) de cet article est remplie. L'une de ces exceptions peut être invoquée par les professionnels de la santé et couvre le cas de figure dans lequel *« le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3 » (article 9 paragraphe (2) lettre (h)), alors que l'exception prévue par l'article 9 paragraphe (2) lettre (b) est mobilisable par les employeurs dans le cas où « le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ».*

Par ailleurs, la CNPD comprend, suite à l'adoption de la loi du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie du Covid-19, qu'il ressort des missions du directeur de la santé ou de son délégué de traiter les données de santé des personnes infectées ou à haut risques d'être infectées en vue de suivre l'évolution de la propagation du virus SARS-CoV-2.

Au contraire, il n'appartiendrait pas à un employeur de se substituer à la direction de la santé en conduisant sa propre investigation concernant l'état de santé ou les contacts de ses employés, ou en établissant son propre registre de « contact tracing », au regard du principe de minimisation des données, énoncé à l'article 5 paragraphe (1) lettre e) du RGPD. Cela n'empêcherait toutefois pas un employeur d'être le cas échéant amené à collaborer et à transmettre toute information pertinente au cas par cas avec la division de l'inspection sanitaire de la direction de la Santé, dans le cadre d'une procédure de traçage des contacts mise en œuvre par cette dernière.

La Commission nationale en conclut que, à défaut de précisions supplémentaires dans le texte du projet de loi sous avis quant aux données de santé qui devraient être transmises, et quant aux traitements de ces signalements par les employeurs, ces derniers ne peuvent alors traiter que les avis d'aptitude ou d'inaptitude à reprendre le travail émis par un professionnel de santé, sans autre précision relative à l'état de santé de l'employé, de la même manière qu'ils traitent d'autres arrêts de maladie. Une collaboration entre les employeurs et la division de l'inspection sanitaire de la direction de la santé pourrait également être envisagée pour la communication d'informations jugées pertinentes par celle-ci.

Cependant, il existe actuellement une incertitude quant à cette interprétation des dispositions actuellement applicables, ne permettant pas aux employeurs de déterminer précisément les données qu'il convient de traiter dans le cadre de la prise de mesure de sécurité et de santé au travail afin de lutter contre la propagation de l'épidémie de COVID-19, ni aux salariés de savoir quelles données ils sont tenus de communiquer à leur employeur. La CNPD estime dès lors que le projet de loi sous avis ne respecte pas les exigences de clarté, de précision et de prévisibilité auxquelles un texte légal doit répondre, conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme[151]. Afin de parer à cette insécurité juridique quant à cette interprétation et d'assurer la conformité du cadre légal luxembourgeois au RGPD et à la jurisprudence européenne, la CNPD suggère aux auteurs du projet de loi de clarifier le type de données personnelles que les salariés devraient communiquer et les obligations des employeurs en ce qui concerne le traitement de ces données.

Ainsi décidé à Esch-sur-Alzette en date du 30 octobre 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

[151] En ce sens, voir M. Besch, « Traitement de données à caractère personnel dans le secteur public », *Normes et légistique en droit public luxembourgeois,* Luxembourg, Promoculture Larcier, 2019, p.469, n°619; Voir entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015.

ANNEXES

5

Deuxième 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°25/2020 du 18 novembre 2020)

Conformément à l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention 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 »), à laquelle se réfère l'article 8 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 (ci-après désignée « 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 la Chambre des députés, 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 des données personnelles* ».

Le présent avis a pour objet les amendements 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, amendements que la Commission des Institutions et de la Révision constitutionnelle (ci-après « la Commission ») a adoptés dans sa réunion du 12 juin 2020.

En date du 16 juillet 2018, la CNPD avait rendu un premier avis au sujet du projet de loi n°6961[152]. En date du 17 décembre 2019, elle a rendu un avis complémentaire.[153]

En date du 13 juillet 2016, la CNPD avait avisé un 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.[154]

En 2013 déjà, la CNPD avait par ailleurs 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.

[152] Délibération n°444/2018 du 16 juillet 2018 https://cnpd.public.lu/fr/decisions-avis/20171/444-pl6961-ANS.html
[153] Délibération n°60/2019 du 17 décembre 2019 https://cnpd.public.lu/fr/decisions-avis/2019/60-autorite-nationale-securite.html
[154] Délibération n°639/2016 du 13 juillet 2016 https://cnpd.public.lu/fr/decisions-avis/2016/SRE.html

Article 28 paragraphe (6) projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité (amendement 9)

L'article 28 paragraphe (6) projeté prévoit ce qui suit :

« (6) Le système informatique par lequel tout accès est opéré est aménagé de sorte que :

1° les membres de l'ANS ne puissent consulter les fichiers auxquels ils ont accès qu'en indiquant leur identifiant numérique personnel, et

2° les informations relatives aux membres de l'ANS ayant procédé à la consultation, ainsi que les informations consultées, la date et l'heure de la consultation sont enregistrées et conservées pendant un délai de cinq ans, afin que le motif de la consultation puisse être retracé. Les données à caractère personnel consultées doivent avoir un lien direct avec les faits ayant motivé la consultation. »

La CNPD estime positif le fait que les fichiers de journalisation seront désormais réglés en détail par le texte dans sa version amendée. Elle suggère encore de prévoir que le motif de la consultation doit être introduit dans le système au moment de la consultation et conservé pendant cinq ans également.

En effet, les informations relatives aux agents ayant procédé à la consultation, les informations consultées, la date et l'heure de la consultation ne permettent pas forcément de retracer le motif jusqu'à cinq ans après la consultation.

Article 29bis projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité (amendement 10)

L'article 29bis projeté prévoit ce qui suit :

« Art. 29bis. – Sécurité des traitements

(1) Toute personne qui agit sous l'autorité du responsable du traitement et qui accède à des données ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu d'obligations légales.

(2) Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

(3) En fonction du risque d'atteinte à la vie privée, ainsi que de l'état de l'art et des coûts liés à leur mise en œuvre, les mesures visées au paragraphe (2) doivent :

(a) empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données (contrôle à l'entrée des installations) ;

(b) empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports) ;

(c) empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées (contrôle de la mémoire) ;

(d) empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation) ;

(e) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès) ;

(f) garantir que puisse être vérifié et constaté l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission (contrôle de la transmission) ;

(g) garantir que puisse être vérifié et constaté a posteriori l'identité des personnes ayant eu accès au système d'information et quelles données ont été introduites dans le système, à quel moment et par quelle personne (contrôle de l'introduction) ;

(h) empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport) ;

(i) sauvegarder les données par la constitution de copies de sécurité (contrôle de la disponibilité).

(4) Quiconque effectue un traitement en violation des règles relatives à la confidentialité ou à la sécurité visées aux paragraphes (1), (2) et (3) est puni d'un emprisonnement de huit jours à six mois et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions des paragraphes (1), (2) et (3) sous peine d'astreinte dont le maximum est fixé par ladite juridiction. »

La Commission nationale note que le texte reprend les termes des articles 22 et 23 de la loi abrogée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et complètera les dispositions actuelles des articles 22, 24 et 28 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.

En revanche, ne sont pas fixés par les textes mentionnés ci-dessus les délais de conservation exacts des fichiers de journalisation y prévus. La CNPD suggère de préciser dans le projet de loi un délai de conservation de 5 ans pour ce qui est des fichiers de journalisation relatifs aux consultations des données dans les systèmes de traitement de données de l'ANS. Il convient de relever que la prescription des délits, (et notamment des infractions pénales prévues par 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, par l'article 29 bis paragraphe (4) projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ou par les articles 458 ainsi que 509-1 et suivants du Code pénal,) est de 5 ans.

Ainsi décidé à Belvaux en date du 18 novembre 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

ANNEXES

5

Avis relatif au projet de règlement grand-ducal fixant les modalités d'enregistrement des établissements des exploitants du secteur alimentaire.

(Délibération n°27/2020 du 2 décembre 2020)

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 désigné 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 ») *« 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 ».*

Par courrier en date du 12 août 2020, Madame la Ministre de la Protection des consommateurs a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal fixant les modalités d'enregistrement des établissements des exploitants du secteur alimentaire (ci-après désigné le « projet de règlement grand-ducal »).

Il ressort de l'exposé des motifs que selon la règlementation européenne, tout exploitant du secteur alimentaire doit faire enregistrer auprès des autorités compétentes chacun des établissements dont il a la responsabilité et qui intervient dans la chaîne alimentaire.

Au niveau national, l'article 6 de la loi du 28 juillet 2018 instaurant un système de contrôle et de sanction relatif aux denrées alimentaires a trait à cet enregistrement en disposant que *« (…) tout exploitant du secteur alimentaire notifie au commissariat [du gouvernement à la qualité, à la fraude et à la sécurité alimentaire], aux fins d'enregistrement, chacun des établissements dont il a la responsabilité et qui mettent en œuvre l'une des étapes de la production, de la transformation et de la distribution de denrées alimentaires. À cet effet, le commissariat est autorisé à exploiter un fichier, et les données y inscrites seront transmises aux administrations chargées du contrôle des denrées alimentaires. »*

Le paragraphe 2 dudit article poursuit que *« [u]n règlement grand-ducal précise les procédures ainsi que les modalités d'enregistrement des établissements visées au paragraphe 1er du présent article. »*

Le projet de règlement grand-ducal s'inscrit dans le cadre de la mise en œuvre de l'article 6 précité, même si, dans les faits, un système de notification informatisé est opérationnel depuis 2016.

La Commission nationale limitera ses observations aux dispositions du projet de règlement grand-ducal sans examiner plus en détail la législation européenne et nationale sur base de laquelle le projet de règlement grand-ducal a été pris.

L'article 3 du projet de règlement grand-ducal énumère les informations que les exploitants du secteur alimentaire doivent notifier au commissariat du gouvernement à la qualité, à la fraude et à la sécurité alimentaire, à savoir (i) l'enseigne commerciale de l'établissement, (ii) l'adresse physique où ont lieu les activités, (iii) les coordonnées de contact et l'adresse de l'exploitant, (iv) les activités liées aux étapes de la production, de la transformation et de la distribution des denrées alimentaires et (v) lorsque l'exploitant est une personne morale, la personne physique désignée comme destinataire des rapports des contrôles officiels et comme interlocuteur en cas d'incidents liés aux denrées alimentaires pour le compte de cette personne morale.

Sur base des informations dont elle dispose, la Commission nationale considère que les catégories de données personnelles à notifier sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, à savoir le contrôle des exploitants du secteur alimentaire[156], de sorte que le principe de minimisation des données posé à l'article 5, paragraphe 1er, lettre c) du RGPD est respecté.

L'article 5 du projet de règlement grand-ducal dispose que le commissariat du gouvernement à la qualité, à la fraude et à la sécurité alimentaire tient un registre des établissements où figurent les données notifiées conformément à l'article 3 et que les données, régulièrement mises à jour, sont conservées pendant une durée maximale de 5 années après la fin des activités liées aux étapes de la production, de la transformation et de la distribution des denrées alimentaires.

La Commission nationale estime qu'au vu du fait que la loi du 28 juillet 2018 instaurant un système de contrôle et de sanctions relatif aux denrées alimentaires prévoit des peines correctionnelles se prescrivant par 5 ans, la limitation de la conservation des données à une durée maximale de 5 années est conforme au principe de limitation de conservation des données personnelles prévu à l'article 5, paragraphe 1er, lettre e) du RGPD.

En ce qui concerne le terme « registre » utilisé à l'article 5 du projet de règlement grand-ducal, la Commission nationale estime qu'il serait préférable d'employer le même terme que celui déjà employé à l'article 6 de la loi précitée du 28 juillet 2018, à savoir « fichier ». Non seulement cette façon de procéder mettrait en exergue le fait qu'il s'agit effectivement du même fichier, mais ce terme présente aussi l'avantage d'être défini par le RGPD[157].

Finalement, la Commission nationale se demande s'il n'y aurait pas une éventuelle incohérence entre la loi du 28 juillet 2018 instaurant un système de contrôle et de sanctions relatif aux denrées alimentaires et le projet de règlement grand-ducal. En effet, l'article 6 de la loi précitée énonce que les données inscrites dans le fichier seront

[156] Même si la finalité du traitement se dégage de la lecture des différents textes normatifs, il pourrait être utile de la rappeler à l'article 1er du projet de règlement grand-ducal.
[157] Article 4, point 6) du RGPD.

transmises aux administrations chargées du contrôle des denrées alimentaires tandis que le projet de règlement grand-ducal, tout en restant muet à ce sujet dans le corps du texte, indique dans son exposé des motifs qu'*« afin d'éviter notamment des doubles emplois et de renforcer l'efficacité des contrôles officiels, il s'avère indispensable d'avoir un registre centralisé des établissements de la chaîne alimentaire ».*

Selon la compréhension de la CNPD, la loi précitée du 28 juillet 2018 ne permet pas aux administrations chargées du contrôle des denrées alimentaires d'accéder directement audit fichier dans la mesure où les données y inscrites leur sont transmises par le commissariat du gouvernement à la qualité, à la fraude et à la sécurité alimentaire. En évoquant un « registre centralisé », les auteurs du projet de règlement grand-ducal semblent toutefois vouloir créer un fichier directement accessible aux administrations chargées du contrôle des denrées alimentaires.

A toutes fins utiles, la Commission nationale se permet de relever que l'accès à des fichiers externes contenant des données à caractère personnel et la transmission de telles données à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi[158]. En cas d'accès direct, la loi devrait notamment énumérer les administrations pouvant accéder au fichier en question, tout comme les finalités de cet accès.

Ainsi décidé à Belvaux en date du 2 décembre 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

[158] V. notamment en ce sens l'avis 6975/5 du Conseil d'État 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 relatif au projet de loi n°7639 modifiant la loi du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement et au projet de règlement grand-ducal abrogeant le règlement grand-ducal du 23 décembre 2016 fixant les mesures d'exécution de la loi du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement.

(Délibération n°28/2020 du 2 décembre 2020)

Conformément à l'article 57, paragraphe (1), 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 ».*

Par courrier en date du 21 juillet 2020, Monsieur le Ministre du Logement a invité la Commission nationale à se prononcer sur le projet de loi modifiant la loi du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement (ci-après le « projet de loi ») et le projet de règlement grand-ducal abrogeant le règlement grand-ducal du 23 décembre 2016 fixant les mesures d'exécution de la loi du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement (ci-après le « projet de règlement grand-ducal »).

A titre de remarque liminaire, il y a lieu de relever que l'article 1er, dernier alinéa, de la loi du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement (ci-après la « loi du 23 décembre 2016 ») continue à renvoyer à la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Or, cette 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. Il conviendrait dès lors de supprimer ce renvoi et de se référer dorénavant à la législation actuellement en vigueur.

I. L'abrogation du règlement grand-ducal

Les auteurs du projet de loi se proposent d'abroger le règlement grand-ducal du 23 décembre 2016 fixant les mesures d'exécution de la loi du 23 décembre 2016 et d'insérer ces dispositions directement dans la loi.

Ainsi, les dispositions du règlement grand-ducal précité se retrouveraient désormais aux articles 4, paragraphe (5), et 5, paragraphe (1), alinéa 2, de la loi du 23 décembre 2016, tel que modifié par le projet de loi.

La CNPD salue une telle modification alors qu'elle l'avait suggérée dans son avis du 25 novembre 2016 relatif au projet de loi n°7054.

Toutefois, vu les autres modifications que les auteurs du projet de loi entendent apporter à la loi du 23 décembre 2016, la Commission nationale se demande s'il est toujours opportun d'insérer dans la loi l'énumération des données à caractère personnel pouvant être échangées entre autorités étatiques. La CNPD y reviendra *infra* au point III. du présent avis.

II. Le changement de terminologie

Les auteurs du projet de loi indiquent dans l'exposé des motifs vouloir profiter de l'occasion *« pour préciser le texte à certains endroits, lequel prévoit maintenant une terminologie plus appropriée »*. Des explications à cet égard ne sont toutefois pas fournies dans l'exposé des motifs ni dans le commentaire des articles.

Or, la Commission nationale se demande si les termes de « données à caractère personnel » et de « fichiers », ne seraient pas plus appropriés que les termes « informations » ou « renseignements », utilisés dorénavant dans l'ensemble du projet de loi, pour des raisons de cohérence avec le RGPD qui définit ces notions dans son article 4, paragraphes (1) et (6). L'utilisation de notions définies par le RGPD permettrait en outre une meilleure compréhension du dispositif sous avis.

En effet, à titre d'exemple, la version initiale du paragraphe (3) de l'article 4, qui utilisait le terme « fichier », permettait une meilleure compréhension du dispositif, alors que la nouvelle terminologie employée, à savoir *« accès aux ~~fichier~~ renseignements du ministre ayant l'Environnement dans ses attributions »* et *« accès aux ~~fichier~~ renseignements du ministre ayant le Logement dans ses attributions »*, est susceptible de porter à confusion.

Par ailleurs, les auteurs du projet de loi précisent à l'article 4, paragraphe (4), tel que modifié par le projet de loi, que les demandeurs et les bénéficiaires d'aides au logement doivent donner leur consentement « explicite ». La Commission nationale se demande ce que les auteurs entendent lorsqu'ils souhaitent préciser le caractère « explicite » du consentement.

En tout état de cause, il y a lieu de rappeler qu'en matière de protection des données, le consentement est défini par l'article 4, paragraphe (11), du RGPD (ce qui implique qu'il doit être « libre, spécifique, éclairé et univoque ») et que son recueil doit s'effectuer conformément aux dispositions légales de l'article 7 du RGPD. Dès lors, le

consentement des demandeurs et des bénéficiaires d'aides au logement devra être donné conformément aux dispositions légales du RGPD, de sorte que le terme explicite peut être considéré comme superflu.

III. La création de nouveaux fichiers

Selon le texte actuellement en vigueur, le ministre ayant le Logement dans ses attributions et le ministre ayant l'Environnement dans ses attributions ont accès à des fichiers externes pour les finalités détaillées dans le texte précité, tandis que le projet de loi sous avis prévoit à l'article 4, paragraphes (1) et (2), que les ministres se voient communiquer par les autorités étatiques, énumérées aux paragraphes précités, certaines données à caractère personnel, « informations nécessaires » ou « renseignements pertinents ».

Faut-il comprendre que, contrairement au système actuel prévoyant une consultation de fichiers externes par le ministre ayant le Logement dans ses attributions et par le ministre ayant l'Environnement dans ses attributions, ces derniers sont désormais destinataires de données issues de tels fichiers ? Les ministres sont-ils dès lors amenés à tenir des fichiers dans lesquels figureront de telles données ?

Si tel devait être le cas, la CNPD tient à réitérer ses observations formulées dans son avis du 25 novembre 2016 relatif au projet de loi n°7054[159] et rappelle que la tenue d'un fichier de données à caractère personnel collectées et traitées par une autorité étatique doit reposer sur une base légale conformément à l'article 6, paragraphe (3) du RGPD.

Cet article 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 définis soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis.

De plus, 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 du RGPD précise encore que 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 et de la Cour européenne des droits de l'Homme[160].

[159] La CNPD avait notamment relever dans son avis du 25 novembre 2016 relatif au projet de loi n°7054 qu'*« [e]n l'absence de consentement de la personne concernée à ce que les ministres compétents vérifient directement dans les fichiers détenus par d'autres administrations les informations nécessaires à l'instruction des demandes d'aides au logement, les personnes concernées disposent en principe d'une alternative consistant à fournir elles-mêmes des pièces justificatives comportant des informations issues desdits fichiers et documentant leur situation administrative. Il en résulte une nécessité d'encadrer au-delà de l'hypothèse d'un consentement préalable des personnes concernées, les cas où les ministres concernés seraient rendus destinataires de données issues de bases de données administratives gérées par d'autres administrations. La CNPD estime essentiel que l'encadrement normatif sur ce point figure dans la loi »*

[160] En ce sens, voir M. Besch, « Traitement de données à caractère personnel dans le secteur public », Normes et légistique en droit public luxembourgeois, Luxembourg, Promoculture Larcier, 2019, p.470, n°619.

En vertu des dispositions précitées, ces bases légales devraient établir des dispositions spécifiques visant à déterminer, entre autres, les types de données traitées, les personnes concernées, les entités auxquelles les données peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

Ainsi, pour que la licéité du traitement dans le secteur public soit assurée, il faut disposer d'un texte normatif national ou supranational qui peut amener une administration ou un service à devoir traiter des données pour remplir ses missions[161]. S'il ne faut pas qu'un texte prescrive spécifiquement un traitement de données, « la finalité du traitement doit cependant être précise, dans la mesure où le texte amenant l'administration à traiter des données doit permettre aux administrés d'en déduire la nature des données et les fins pour lesquelles celles-ci sont utilisées »[162]. La Commission nationale estime donc indispensable, dans l'hypothèse où les ministres susvisés, tiennent un ou plusieurs fichiers, en tant que responsables du traitement, que le présent projet de loi prévoit les dispositions légales portant création de tels fichiers. Celles-ci devront contenir les éléments cités ci-avant.

Dans la mesure où les dispositions de l'article 3 alinéa 2 de la loi du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement[163] semblent d'ores et déjà prévoir la tenue d'un fichier par le ministre ayant le Logement dans ses attributions, celles-ci devraient être complétées alors qu'elles sont formulées de manière trop vague. Lesdites dispositions devraient notamment préciser que le ministre précité aura la qualité de responsable du traitement et que le fichier contiendra, outre les données actuellement visées par l'article 3 de la loi précitée, les données reçues par ledit ministre par les administrations visées à l'article 4, tel que modifié, par le projet de loi.

Par ailleurs, des dispositions similaires concernant la tenue d'un fichier par le ministre ayant l'Environnement dans ses attributions devraient également être insérées à l'article 3 précité alors que cela n'est pas précisé actuellement par le texte sous avis.

En tout état de cause, si la volonté des auteurs du projet de loi est de prévoir une communication de données aux ministres précités par les administrations visées aux paragraphes (1) et (2) de l'article 4 précité, alors cela devrait clairement être reflété dans l'ensemble du projet de loi.

Ainsi, il conviendrait d'adapter en conséquence la terminologie utilisée à l'article 4, paragraphe (4), et à l'article 5, paragraphe (1), tels que modifiés par le projet de loi, alors que ces articles continuent notamment à faire respectivement référence à l'*« accès aux renseignements du registre national et du répertoire général »* et aux *« accès par les ministres aux renseignements à partir des fichiers énumérés à l'article 4 (…) »*.

IV. L'échange de données entre le ministre ayant le Logement dans ses attributions et le ministre ayant l'Environnement dans ses attributions

[161] M. Besch, « Traitement de données à caractère personnel dans le secteur public », Normes et légistique en droit public luxembourgeois, Luxembourg, Promoculture Larcier, 2019, p.470, n°619.
[162] M. Besch, « Traitement de données à caractère personnel dans le secteur public », Normes et légistique en droit public luxembourgeois, Luxembourg, Promoculture Larcier, 2019, p.470, n°619.
[163] L'article 3 alinéa 2 de la loi du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement dispose que : *« Après la collecte et la saisie des demandes d'aides relatives au logement et des pièces y relatives, les données à caractère personnel sont transférées vers des supports de données sûrs auxquels l'agent du ministre ayant le Logement dans ses attributions ayant effectué la collecte et la saisie n'a pas accès »*.

L'article 4, paragraphe (3), tel que modifié par le projet de loi, maintient un échange de données entre le ministre ayant le Logement dans ses attributions et le ministre ayant l'Environnement dans ses attributions par le biais d'un accès respectif à leurs fichiers.

Cependant, les catégories de données sur lesquels portent cet échange ne sont pas précisées de sorte que la Commission nationale n'est pas à même de se prononcer sur le caractère nécessaire et proportionné de l'échange de données tel que visé au paragraphe (3) précité.

Il conviendrait dès lors que le projet de loi indique *a minima* les catégories de données qui seraient échangées entre lesdits ministres.

En outre, dans la mesure où le projet de loi prévoit une communication spécifique de données issues de fichiers administratifs pour chacun des ministres précités, il y a lieu d'attirer l'attention des auteurs du projet de loi sur le fait que cet échange de données ne doit pas permettre aux ministres d'obtenir de manière indirecte des données à caractère personnel issues de fichiers d'autorités étatiques pour lesquels ils n'ont pas accès en vertu du projet de loi sous avis.

V. La communication de « renseignements » par d'autres autorités

Suivant l'exposé des motifs, le projet de loi sous avis entend prévoir dans la loi du 23 décembre 2016 *« dans quelle mesure et sous quelles conditions le ministère du Logement peut obtenir la communication de renseignements de la part de l'Administration des contributions directes respectivement de la Caisse pour l'avenir des enfants, lesquelles ne figurent pas encore parmi les autorités énumérées à l'article 4 de la prédite loi de 2016 (…) ».*

Il y a lieu de constater que l'article 4, paragraphe (1), point 1°, tel que modifié par le projet de loi, énumère les données personnelles pouvant être transmises par l'Administration des contributions directes au ministre ayant le Logement dans ses attributions.

De telles précisions ne sont toutefois pas apportées pour les données qui seraient transmises au ministre ayant le Logement dans ses attributions et au ministre ayant l'Environnement dans ses attributions en vertu des paragraphes (1), point 2° à 4° et (2) de l'article 4, tel que modifié par le projet de loi.

Cependant, l'article 4, paragraphe (5), tel qu'issu du projet de loi, qui est la reprise de l'article 1er du règlement grand-ducal du 23 décembre 2016 fixant les mesures d'exécution de la loi du 23 décembre 2016, énumère les catégories de données à caractère personnel pouvant être communiquées « à partir des fichiers énumérés aux paragraphes 1er et 2 » aux ministres précités, sans préciser quelles autorités transmettent quelles données à quel ministre.

La Commission nationale se demande, dès lors, comment s'articulent les dispositions spécifiques de l'article 4, paragraphe (1), point 1° avec celles générales de l'article 4, paragraphe (5).

Ainsi, dans un souci de cohérence de la structure interne de l'article 4, tel que modifié par le projet de loi, il serait judicieux que les auteurs du projet de loi précisent pour chaque communication de données visée aux paragraphes (1) et (2) de l'article précité quelles sont les catégories qui pourraient être transmises aux ministres et de supprimer en conséquence le paragraphe (5) de l'article 4, dont les dispositions deviendraient superfétatoires.

Finalement, ne serait-il pas plus pertinent de prévoir que les données d'identification des personnes concernées qui seraient transmises aux ministres afin qu'ils en vérifient l'authenticité et l'exactitude ne soient communiquées que par l'administration qui tient le registre national au sens de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, plutôt que de prévoir que ces données soient communiquées par l'Administration des contributions directes ?

Ainsi décidé à Belvaux en date du 2 décembre 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

Avis relatif à l'avant-projet de loi relative à la reconnaissance des qualifications professionnelles dans le domaine de la navigation intérieure et portant modification de la loi modifiée du 28 juillet 1973 portant création d'un service de la navigation.

(Délibération n°29/2020 du 17 décembre 2020)

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 ».*

Par courrier en date du 18 août 2020, Monsieur le Ministre de la Mobilité et des Travaux publics a invité la Commission nationale à se prononcer sur l'avant-projet de loi relative à la reconnaissance des qualifications professionnelles dans le domaine de la navigation intérieure et portant modification de la loi modifiée du 28 juillet 1973 portant création d'un service de la navigation (ci-après l'« avant-projet de loi »).

L'avant-projet de loi a notamment pour objet de transposer en droit national la directive (UE) 2017/2397 du Parlement européen et du Conseil du 12 décembre 2017 relative à la reconnaissance des qualifications professionnelles dans le domaine de la navigation intérieure et abrogeant les directives du Conseil 91/672/CEE et 96/50/CE (ci-après la « directive »). La directive vise à mettre en place un cadre commun en matière de reconnaissance des qualifications professionnelles minimales dans le domaine de la navigation intérieure.

La directive est complétée par la directive déléguée (UE) 2020/12 de la Commission du 2 août 2019 en ce qui concerne les normes relatives aux compétences et aux connaissances et aptitudes correspondantes, aux épreuves pratiques, à l'agrément de simulateurs et à l'aptitude médicale, par le règlement d'exécution (UE) 2020/182 de la Commission du 14 janvier 2020 sur les modèles relatifs aux qualifications professionnelles dans le domaine de la navigation intérieure et par le règlement délégué (UE) 2020/473 de la Commission du 20 janvier 2020 en ce qui concerne les normes applicables aux bases de données relatives aux certificats de qualification de l'Union, aux livrets de service et aux livres de bord.

ANNEXES

5

Dans la mesure où l'avant-projet de loi sous avis transpose en droit national la directive, la Commission nationale limitera ses observations aux dispositions légales concernant la mise en œuvre concrète de cette directive au Luxembourg.

Le présent avis traitera des questions relatives aux aspects de la protection des données à caractère personnel soulevées par les articles des chapitres 3 et 4 de l'avant-projet de loi.

I. Sur les traitements de données effectués par le ministre

Il ressort de la lecture de l'avant-projet de loi que le ministre ayant les transports dans ses attributions (ci-après le « ministre ») collectera et traitera des données (i) lors de la délivrance, du renouvellement et de la suspension, respectivement du retrait des certificats de qualification de l'Union et des autorisations spécifiques[164], (ii) lors de l'accès à des fichiers étatiques[165] et (iii) lors de la tenue de registres tels que visés par l'article 20 de l'avant-projet de loi.

Avant d'examiner plus en détail les traitements effectués à ces occasions (points B à D), la Commission nationale formule quelques observations d'ordre général (point A ci-dessous).

A. Considérations générales

Tout d'abord, il y a lieu de relever que l'article 19 intitulé « Protection des données à caractère personnel » indique notamment que le RGPD s'applique aux traitements de données à caractère personnel prévus par la loi[166], précise les finalités pour lesquelles les données seront traitées[167], se réfère aux droits des personnes concernées[168] et précise que le ministre a la qualité de responsable du traitement[169].

1. Sur la référence au RGPD (article 19 paragraphes (1) et (3) de l'avant-projet de loi)

Bien que le paragraphe (1) de l'article 19 soit une reprise littérale du paragraphe (1) de l'article 24 de la directive, la CNPD se demande s'il est nécessaire, voire opportun, de prévoir que le RGPD s'applique aux traitements de données à caractère personnel prévus par l'avant-projet de loi alors que le RGPD est, en tant que règlement européen, obligatoire dans tous ses éléments et directement applicable au Luxembourg.

En outre, le paragraphe (3) de l'article 19 de l'avant-projet de loi reprend le libellé de l'article 24 paragraphe (4) de la directive en disposant que les personnes dont les données sont traitées sont préalablement informées de ce traitement et qu'elles ont le droit d'accéder à leurs données personnelles et de disposer d'une copie de ces données, sur demande, à tout moment.

[164] Articles 8 et suivants.
[165] Article 19 paragraphe (5).
[166] Article 19 paragraphe (1).
[167] Article 19 paragraphe (2).
[168] L'article 19 paragraphe (3).
[169] L'article 19 paragraphe (4).

La CNPD se demande si cette disposition ne serait pas superfétatoire par rapport aux dispositions qui sont déjà prévues par le RGPD en ce qui concerne le droit à l'information des personnes concernées[170] ainsi que le droit d'accès des personnes concernées[171].

A toutes fins utiles, la Commission nationale se permet d'attirer l'attention des auteurs de l'avant-projet de loi sur la problématique liée au fait de reproduire partiellement ou intégralement le texte d'un règlement européen dans l'ordre juridique interne. En effet, le Conseil d'État rappelle régulièrement dans ses avis la jurisprudence de la Cour de justice de l'Union européenne selon laquelle les États membres ne doivent pas entraver l'applicabilité directe des règlements ni en dissimuler la nature européenne[172].

2. Sur les finalités des traitements (article 19 paragraphe (2) de l'avant-projet de loi)

Il y a lieu de féliciter les auteurs de l'avant-projet de loi sur le fait qu'ils aient précisé les finalités des traitements de données à caractère personnel.

Cependant, et bien que ces dispositions soient une reprise du libellé de l'article 24 paragraphe (3) de la directive, la Commission nationale regrette que celles-ci ne soient pas plus détaillées, notamment en fonction des différents traitements effectués par le ministre. Ceci vaut tout particulièrement pour l'accès par le ministre aux données issues de fichiers tenus par d'autres administrations étatiques.

La CNPD reviendra ultérieurement sur ce point.

3. Sur la désignation du responsable du traitement

Enfin, en ce qui concerne l'article 19 paragraphe (4), qui est un ajout par rapport à la directive, la CNPD se demande la raison d'être de cette disposition alors qu'il ressort d'ores et déjà des articles 8, 9, 10, 11, 18, 19, 20, 21 et 23 de l'avant-projet de loi que le ministre a la qualité de responsable du traitement pour les traitements de données à caractère personnel découlant desdits articles.

Par ailleurs, la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel à laquelle est faite référence 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. Il conviendrait dès lors de se référer à la législation actuellement en vigueur, à savoir l'article 4, point 7) du RGPD.

B. Sur les traitements mis en œuvre dans le cadre de la délivrance, du renouvellement, de la suspension et du retrait des certificats de qualification de l'Union et des autorisations spécifiques

[170] Articles 13 et 14 du RGPD.
[171] Article 15 du RGPD.
[172] V. par. ex. l'avis du Conseil d'État du 17 juillet 2020 sur le projet de loi n°7537 relatif à certaines modalités d'application et à la sanction du règlement (UE) n°2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne

ANNEXES

5

En vertu des articles 8 et suivants de l'avant-projet de loi, la CNPD comprend que le ministre collecte des données à caractère personnel dans le cadre de la délivrance, du renouvellement, de la suspension et du retrait des certificats de qualification de l'Union et des autorisations spécifiques.

1. Sur la condition d'honorabilité (article 8 paragraphe (1) lettre d) de l'avant-projet de loi)

Même si l'article 8 de l'avant-projet de loi constitue une reprise quasi-fidèle de l'article 11 de la directive, il y a lieu de constater qu'une condition supplémentaire a été prévue au paragraphe (1) lettre d). En effet, l'avant-projet de loi indique que les demandeurs doivent fournir au ministre les « pièces justificatives » établissant de manière satisfaisante qu'ils satisfont aux critères d'honorabilité.

Ainsi, le demandeur, afin d'établir son honorabilité, devra fournir un *« extrait de casier judiciaire récent ou un document équivalent du lieu de résidence habituelle ne renseignant pas une condamnation pénale coulée en force de chose jugée prononçant une peine d'emprisonnement d'au moins six moins pour vol, escroquerie, abus de confiance, atteinte volontaire à l'intégrité de la personne, agression sexuelle ou infraction à la législation sur les stupéfiants ou conduite en état d'ivresse ou sous l'influence d'alcool »*. Or, cette condition n'est pas une condition requise par la directive.

Les auteurs de l'avant-projet de loi précisent que la disposition sous avis a été ajoutée *« en raison de l'approche équivalente dans le régime rhénan et afin de maintenir un haut niveau de qualité »*. Cependant, le régime rhénan applicable au personnel de la navigation du Rhin, auquel les auteurs de l'avant-projet de loi font référence[173], est un régime distinct de la directive et n'est pas régi par celle-ci. Dès lors, la CNPD se demande s'il est pertinent de prévoir cette condition supplémentaire prévue par une organisation internationale. En ajoutant une telle condition, l'avant-projet de loi sous avis ne procèderait-il pas à une transposition incorrecte de la directive ?

En outre, la Commission nationale n'est pas en mesure d'apprécier, sur base des commentaires des auteurs de l'avant-projet de loi précités, si la collecte de telles données respecte le principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre c) du RGPD. Les auteurs de l'avant-projet de loi devraient, en effet, expliquer les raisons pour lesquelles ils estiment que la collecte de telles données sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Par ailleurs, il y a lieu d'attirer l'attention des auteurs de l'avant-projet de loi sur le fait que dans l'ordre juridique luxembourgeois, la communication des informations relatives à des décisions de justice se fait par la délivrance d'extraits de casier judiciaire conformément à la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire (ci-après la « loi du 29 mars 2013 »). Cette loi porte création de plusieurs bulletins avec une ventilation des inscriptions se trouvant sur les bulletins respectifs. La Commission nationale recommande dès lors de préciser dans l'avant-projet de loi quel bulletin les demandeurs devront fournir au ministre[174]. Par ailleurs, il serait utile de

[173] Le règlement relatif au personnel de la navigation sur le Rhin adopté par la Commission Centrale pour la Navigation du Rhin.
[174] Au vu des condamnations énumérées à l'article 8 paragraphe (1) lettre d) de l'avant-projet de loi, la CNPD estime que seuls les bulletins Nos 2 et 3 sont susceptibles d'être visés par les auteurs de l'avant-projet de loi.

préciser ce qu'il faut entendre par un extrait de casier judiciaire « récent », en disposant par exemple que l'extrait doit dater de moins de 1 mois.

Au cas où le bulletin N°2 serait visé par l'article 8 paragraphe (1) lettre d) de l'avant-projet de loi, il y a lieu de noter que ce bulletin n'est pas délivré à la personne concernée elle-même mais, sous certaines conditions, aux autorités publiques énumérées à l'article 8 de la loi du 29 mars 2013, respectivement à l'article 1er du règlement grand-ducal modifié du 23 juillet 2016 fixant la liste des administrations et personnes morales de droit public pouvant demander un bulletin N°2 ou N°3 du casier judiciaire avec l'accord écrit ou électronique de la personne concernée (ci-après le « règlement grand-ducal du 23 juillet 2016 »).

Ainsi, il ressort de l'article 1er, point 1) du règlement grand-ducal du 23 juillet 2016 que le « ministre ayant les Transports dans ses attributions » peut obtenir la copie d'un bulletin N°2 « *pour l'instruction de toute demande d'agrément, de licence ou de permis adressée à un service de sa compétence* ». La Commission nationale se demande si la délivrance de certificats de qualifications de l'Union pourrait être visée par cette disposition.

En ce qui concerne le bulletin N°3, celui-ci peut être délivré à la personne concernée elle-même. L'article 8-1 de la loi du 29 mars 2013 prévoit toutefois également la possibilité de délivrer ce bulletin à des tiers, dont notamment les administrations et personnes morales de droit public énumérées par le règlement grand-ducal du 23 juillet 2016. Il y a lieu de noter que le ministre ayant les transports dans ses attributions ne figure pas parmi les autorités publiques y énumérées.

Au regard du libellé de l'article 8 paragraphe (1) lettre d) de l'avant-projet de loi, la Commission nationale comprend qu'il appartient au demandeur de fournir au ministre un extrait du casier judiciaire et que l'avant-projet de loi ne prévoit pas la possibilité pour le ministre de se voir délivrer directement, dans les conditions prévues par la loi du 29 mars 2013 et le règlement grand-ducal du 23 juillet 2016, le bulletin en question.

Au vu de ce qui précède, il serait opportun que des clarifications quant à l'articulation des dispositions de la loi du 29 mars 2013 et du règlement grand-ducal du 23 juillet 2016, d'une part, avec l'article 8 paragraphe (1) lettre d) de l'avant-projet de loi, d'autre part, soient apportées par les auteurs de l'avant-projet de loi.

A toutes fins utiles, il y a lieu de relever que le projet de loi n°7691, déposé le 2 novembre 2020, a pour objet de préciser les différentes procédures de « contrôle d'honorabilité » actuellement prévues dans plusieurs textes de loi et qui relèvent de la compétence du ministre de la Justice[175]. Les dispositions de l'avant-projet de loi relatives à l'honorabilité ne seraient, dès lors, pas susceptibles d'être visées par le projet précité. Cependant et si tel ne devait pas être le cas, ne faudrait-il pas adapter le projet de loi n°7691 afin d'y intégrer les dispositions relatives à l'honorabilité qui figurent dans l'avant-projet de loi sous avis ?

[175] Projet de loi portant modification 1° du Code de procédure pénale 2° du Nouveau Code de procédure civile 3° de la loi du 7 juillet 1971 portant en matière répressive et administrative, institution d'experts, de traducteurs et d'interprètes assermentés et complétant les dispositions légales relatives à l'assermentation des experts, traducteurs et interprètes 4° de la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat 5° de la loi modifiée du 20 avril 1977 sur les jeux de hasard et les paris sportifs 6° de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire 7° de la loi modifiée du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif 8° de la loi du 30 décembre 1981 portant indemnisation en cas de détention préventive inopérante 9° de la loi modifiée du 15 mars 1983 sur les armes et munitions 10° de la loi modifiée du 2 mars 1984 relative à l'indemnisation de certaines victimes de dommages corporels résultant d'une infraction et à la répression de l'insolvabilité frauduleuse 11° de la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice 12° de la loi du 31 janvier 1998 portant agrément des services d'adoption et définition des obligations leur incombant 13° de la loi du 6 mai 1999 relative à la médiation pénale et portant modification de différentes dispositions a) de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire, b) du code des assurances sociales 14° de la loi du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance 15° de la loi modifiée du 7 juin 2012 sur les attachés de justice.

2. Sur l'aptitude médicale (article 8 paragraphe (1) lettre c))

Il y a lieu de rappeler que les données personnelles qui seraient collectées par le ministre afin d'attester qu'un candidat présente les aptitudes médicales requises sont à qualifier de données dites « sensibles » au sens de l'article 9 du RGPD. Celles-ci sont en effet relatives à la santé des candidats. Les traitements de telles données requièrent dès lors une protection spécifique et sont soumis à des exigences plus strictes.

Afin d'établir que les demandeurs satisfont aux normes d'aptitudes, ces derniers doivent délivrer un certificat médical sur base de la procédure visée par l'article 18 de l'avant-projet de loi.

L'article 18 prévoit notamment que les demandeurs *« démontrent leur aptitude médicale en présentant au ministre un certificat médical valable délivré par un médecin reconnu par le ministre, sur la base d'un examen confirmant l'aptitude médicale »*. La Commission nationale comprend dès lors que le ministre ne se verra transmettre qu'un certificat confirmant ou non l'aptitude médicale du demandeur.

Par ailleurs, les normes d'aptitude médicale précisant les exigences relatives à l'aptitude médicale, notamment en ce qui concerne les tests que les médecins doivent pratiquer sont détaillées à l'annexe III de la directive ainsi qu'à l'annexe IV de la directive déléguée (UE) 2020/12 de la Commission du 2 août 2019 complétant la directive.

Cet article est une transposition fidèle de l'article 23 de la directive et n'appelle pas de commentaires de la part de la CNPD.

3. Sur la vérification de l'authenticité et validité des documents

Il ressort des articles 8 et 9 de l'avant-projet de loi que le ministre *« vérifie l'authenticité et la validité des documents fournis par les demandeurs »*. L'article 23 paragraphe (1) de l'avant-projet de loi dispose encore que *« [l]e ministre prend les mesures appropriées pour prévenir la fraude et d'autres pratiques illégales concernant les certificats de l'Union, les livrets de service, les livrets de bord, les certificats médicaux et les registres prévus par la présente loi »*.

La Commission nationale comprend que de telles mesures visent à prévenir la fraude et d'autres pratiques illégales. Néanmoins, en l'absence de précision dans le commentaire des articles, elle se demande par quels moyens le ministre entend vérifier l'authenticité et la validité des documents. La vérification de l'authenticité et de la validité des documents se fait-elle au moyen d'accès à des fichiers étatiques, tels que ceux énumérés au paragraphe (5) de l'article 19 de l'avant-projet de loi ? Dans l'affirmative, cela devrait figurer clairement dans l'avant-projet de loi.

Si l'accès à d'autres fichiers étatiques que ceux énumérés à l'article précité devait être prévu alors cela devrait être clairement déterminé et encadré par l'avant-projet de loi.

4. Sur l'article 21 intitulé « Suivi »

L'article 21 de l'avant-projet de loi prévoit la création d'un système de suivi notamment en ce qui concerne la *« délivrance et la mise à jour des certificats de qualification de l'Union, des livrets de service et des livres de bord »*. Cet article est une reprise quasi-littérale de l'article 27 de la directive.

La Commission nationale comprend que ce système de suivi est visé à l'article 11 paragraphe (1) de l'avant-projet de loi qui dispose que *« [l]orsque des éléments laissent à penser que les exigences relatives aux certificats de qualification ou autorisations spécifiques ne sont plus satisfaites, le ministre lorsqu'il a délivré le certificat ou l'autorisation spécifique effectue toutes les évaluations nécessaires et, le cas échéant, retire ces certificats ou cette autorisation spécifique »*.

Le paragraphe (2) de l'article précité dispose encore que *« [l]e ministre peut suspendre temporairement un certificat de qualification de l'Union, dès lors qu'il estime que cette suspension est nécessaire pour des raisons de sécurité ou d'ordre public »*.

Ainsi, s'il ressort des dispositions mentionnées ci-avant que le ministre semble opérer un suivi des certificats de qualification ou autorisations spécifiques, les modalités d'un tel suivi ne sont toutefois pas précisées dans l'avant-projet de loi.

Or, dans un tel contexte, la CNPD se demande quelles seraient les informations qui seraient transmises le cas échéant au ministre. En outre, est-ce que le ministre se voit communiquer directement des données à caractère personnel par la Police grand-ducale ou le Ministère public lorsqu'une suspension d'un certificat de l'Union *« est nécessaire pour des raisons de sécurité ou d'ordre public » ?*

Dès lors, il conviendrait de préciser les modalités d'un tel suivi, et plus particulièrement quelles catégories de données à caractère personnel seraient communiquées, le cas échéant, au ministre et par quelles administrations.

C. Sur l'accès aux fichiers visés par l'article 19 paragraphe (5) de l'avant-projet de loi

L'article 19 paragraphe (5) de l'avant-projet de loi prévoit que le ministre peut accéder au :

- registre national des personnes morales créé par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales (ci-après le « registre nationale des personnes morales ») ;
- registre national des personnes physiques créé par la loi du 19 juin 2013 relative à l'identification des personnes physiques (ci-après le « RNPP ») ;
- fichier exploité par le ministre ayant l'enregistrement et des domaines dans ses attributions ; et

- registre des entreprises qui exercent une activité visée à la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales (ci-après le « registre des entreprises »).

Il y a lieu de relever que les dispositions de ce paragraphe ne transposent pas un article de la directive et ont été ajoutées par les auteurs de l'avant-projet de loi afin *« de rendre opérationnelles les dispositions de la loi »*. La CNPD se félicite dès lors que ces derniers précisent pour chacun des fichiers précités quelles sont les catégories de données qui pourront être transmises au ministre et pour quelles finalités. Néanmoins, tel qu'exposé ci-après, certaines précisions mériteraient d'être apportées.

En outre, il convient de rappeler que l'accès auxdits fichiers ne doit pas permettre au ministre d'obtenir de manière indirecte des données à caractère personnel issues d'autres fichiers d'autorités étatiques pour lesquels il n'a pas accès en vertu de l'avant-projet de loi sous avis. Dans l'affirmative, une telle communication de données entre ministères ou administrations devrait être précisée dans l'avant-projet de loi sous avis.

1. Sur les finalités

En tant que remarque liminaire, la CNPD suppose qu'une erreur matérielle s'est glissée au début de l'article 19 paragraphe (5) de l'avant-projet de loi en ce qu'il se réfère au paragraphe (1) et non pas au paragraphe (2) de l'article 19.

Les auteurs de l'avant-projet de loi précisent que les fichiers peuvent être consultés pour *« la mise en œuvre, le contrôle de l'application et l'évaluation de la présente loi »* et l' *« échange d'informations entre les autorités ayant accès à la base de données visées à l'article 20 et la Commission européenne »*. Or, les finalités ne sont pas rédigées avec suffisamment de précision de sorte que la CNPD n'est pas en mesure d'apprécier si les données transmises sont, conformément au principe de minimisation des données consacré à l'article 5 paragraphe (1) lettre c) du RGPD, réellement nécessaires à la réalisation desdites finalités.

La Commission nationale se demande si ces accès ne permettraient pas plutôt au ministre de vérifier l'authenticité des pièces justificatives fournies sur base des articles 8 et suivants de l'avant-projet de loi[176]. L'accès à ces fichiers est-il, en outre, nécessaire afin de prévenir la fraude ou d'autres pratiques illégales telles que visées à l'article 23 de l'avant-projet de loi ?

Des précisions à ce sujet mériteraient d'être apportées.

2. Sur les catégories de données à caractère personnel

[176] Voir les développements ci-dessus au point I. A. 3. du présent avis.

Tout d'abord, il y a lieu de constater que le ministre se voit communiquer des données à caractère personnel ainsi que des données concernant des personnes morales. A ce titre, il convient de relever que le considérant 14 du RGPD dispose que le RGPD *« (…) ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale »*.Toutefois, des informations ayant trait à des personnes morales peuvent, le cas échéant, concerner des personnes physiques (par exemple : si elles incluent le nom du gérant de la société) et doivent dès lors être considérées comme des données à caractère personnel.

Ainsi, le RGPD ne s'appliquera qu'aux données à caractère personnel qui seraient communiquées au ministre.

a) Sur l'accès au registre national des personnes morales :

L'article 19, paragraphe (5) lettre a) prévoit que le ministre peut accéder aux données issues du registre national des personnes morales créé par la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales afin d'obtenir les informations d'identifications des entreprises de transport fluvial, dont notamment au *« numéro d'identification national »* et à l'*« adresse »*.

Selon la compréhension de la CNPD, le registre national des personnes morales ne contient en principe pas de données à caractère personnel de sorte que le RGPD n'est pas d'application. Néanmoins, afin d'éviter toute confusion, il serait souhaitable que les auteurs du projet de loi utilisent les termes tels qu'ils sont employés par la loi précitée du 30 mars 1979. Si la Commission nationale ne se méprend pas, la correcte terminologie est *« numéro d'identité »* et *« siège social »*.

b) Sur l'accès au RNPP :

En vertu de l'article 19 paragraphe (5) lettre b), le ministre a accès au registre national des personnes physiques *« afin d'obtenir les informations d'identification du membre d'équipage de pont (…) »* telles que les noms et prénom, le numéro d'identification national, la nationalité et le pays de résidence.

Il convient de rappeler que l'accès au RNPP par le ministre devrait par ailleurs s'effectuer conformément à la procédure prévue par l'article 10 de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques ainsi que les articles 5 à 7 du règlement grand-ducal du 28 novembre 2013 fixant les modalités d'application de la loi précitée.

c) Sur l'accès au fichier renseignant sur les bateaux immatriculés au Luxembourg

L'avant-projet de loi prévoit que le ministre peut accéder aux données issues du fichier exploité par le ministre ayant l'enregistrement et des domaines dans ses attributions renseignant sur les bateaux immatriculés au Luxembourg.

Plus précisément, le ministre peut accéder aux *« données nécessaires à l'identification des bâtiments, propriétaire, détenteur, adresse, échéances ».*

La Commission nationale estime que l'avant-projet de loi devrait faire référence à la loi portant création du fichier en question. A défaut de cette indication, elle n'est pas en mesure de se prononcer sur l'accès audit fichier.

d) Sur l'accès au registre des entreprises

La CNPD comprend qu'il s'agit du registre visé à l'article 32 paragraphe (1) de la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales et que le ministre ne se verra accorder qu'un accès limité audit registre. La Commission nationale se félicite dès lors que les auteurs de l'avant-projet de loi ne prévoient qu'un accès limité audit registre.

Cependant, en ce qui concerne les informations relatives à la capacité financière de l'entreprise de transport fluvial, quelles catégories de données à caractère personnel seraient, le cas échéant, transmises au ministre ? Des précisions à ce sujet mériteraient d'être apportées par les auteurs de l'avant-projet de loi. Par ailleurs, et afin d'éviter toute confusion, il conviendrait également de préciser ce que recouvre le terme *« adresses »*. S'agit-il du siège social de l'entreprise de transport fluvial ou de l'adresse de ses représentants légaux ?

D. Sur les registres tenus par le ministre

L'article 20 de l'avant-projet de loi transpose l'article 25 de la directive et a notamment pour objet de prévoir la création de registres qui seront tenus par le ministre. En effet, le paragraphe (1) dudit article dispose que le ministre tient des registres *« pour les certificats de qualification de l'Union, livrets de service et livres de bord délivrés sous son autorité (…) et, le cas échéant, pour les documents reconnus en vertu de l'article 7, paragraphe 2, qui ont été délivrés, renouvelés, suspendus ou retirés, qui ont été déclarés perdus, volés ou détruits, ou qui ont expiré (…) ».*

La CNPD comprend à la lecture du paragraphe précité que le ministre tient un registre pour les certificats de qualification de l'Union, un autre registre pour les livrets de service et un troisième registre pour les livres de bords. Le paragraphe énumère en outre les catégories de données qui seraient collectées par le ministre pour chacun des registres.

Cependant, la Commission nationale se demande si ces registres ne constitueront pas un seul et même traitement de données relatif à ce registre, alors que les auteurs de l'avant-projet de loi mentionnent dans leurs commentaires *« la tenue du registre national »* et se réfèrent dans le corps du texte à plusieurs reprises au *« registre visé à l'article 20, paragraphe 1er »*[177]. Ainsi, il est recommandé de clarifier dans l'avant-projet de loi s'il s'agit d'un seul registre ou, par contre, de plusieurs traitements de données ou registres séparés tenus par le ministre.

[177] V. notamment les articles 19, paragraphe (6) et 20, paragraphe (3) de l'avant-projet de loi.

1. Sur les catégories de données à caractère personnel

L'article 20 paragraphe (1) de l'avant-projet de loi énumère les données à caractère personnel que les registres tenus par le ministre contiennent. De ce point de vue, cet article, qui est une transposition fidèle de l'article 25 paragraphe (1) de la directive, ne soulève pas de commentaires de la CNPD.

Il y a toutefois lieu de relever qu'outre les données énumérées au paragraphe (1) de l'article 20 précité, la CNPD comprend que les données issues des fichiers énumérés au paragraphe (5) de l'article 19 seront conservées dans ces registres. En effet, l'article 19 paragraphe (6) prévoit que *« la consultation et la réception des données de ces banques de données peut se faire de façon automatique dans le registre visé à l'article 20, paragraphe 1er »*.

Il convient encore de relever que le ministre sera également amené à collecter et à traiter des données à caractère personnel dans le cadre de la procédure de délivrance des certificats de qualification de l'Union et des autorisations spécifiques visés par les articles 8 et 9. La CNPD comprend que seules les données figurant sur les certificats de qualification de l'Union seront contenues dans les registres et non pas les pièces justificatives fournies par les demandeurs de certificats à l'appui de leur demande.

En tout état de cause, si les registres tenus par le ministre devaient contenir d'autres données que celles énumérées à l'article 20 paragraphe (1), alors cela devrait être reflété clairement dans l'avant-projet de loi.

2. Sur les mesures de sécurité encadrant l'accès aux registres

Conformément à l'article 5 paragraphe (1) lettre f) du RGPD, les données à caractère personnel doivent être *« traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) »*.

De plus, l'article 32 du RGPD dispose que *« le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »*. Pareilles mesures doivent être mises en œuvre afin d'éviter notamment des accès non-autorisés aux données ou des fuites de données.

Ainsi, la Commission nationale se félicite que les auteurs de l'avant-projet de loi aient précisé les modalités d'accès aux registres tenus par le ministre de même qu'ils aient prévu une traçabilité des accès auxdits registres.

Par ailleurs, la dernière phrase de l'article 19 paragraphe (4) de l'avant-projet de loi prévoit que *« [s]eules sont habilitées à avoir accès aux données les personnes qui en ont besoin dans l'exercice de leur fonction et de leurs*

tâches professionnelles ». Selon la compréhension de la CNPD, cette disposition s'applique à l'ensemble des traitements prévus par l'avant-projet de loi, partant également à l'accès aux registres visé à l'article 20 paragraphe (1).

3. Sur la durée de conservation des données à caractère personnel

Selon l'article 5 paragraphe (1) lettre e) du RGPD, les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées.

L'alinéa 1 du paragraphe (3) de l'article 20 de l'avant-projet de loi transpose de manière fidèle l'article 25 paragraphe (3) de la directive. L'alinéa 2 du paragraphe (3) de l'article 20 de l'avant-projet de loi est un ajout par rapport à la directive. Cet alinéa donne des précisions quant à la date de suppression de certaines catégories de données.

Ainsi, il est prévu que *« les données relatives à un bateau sont supprimées du registre visé au paragraphe 1er lorsque ce bâtiment est démantelé »* et que *« les données relatives à un livret de service ou un certificat de qualification sont supprimées du registre visé au paragraphe 1er lorsque la personne concernée est décédée »*.

La CNPD se demande si une telle durée de conservation des données à caractère personnel, notamment jusqu'au décès de la personne concernée, est proportionnée et nécessaire. En effet, est-il nécessaire de conserver jusqu'au décès d'une personne les données la concernant et figurant sur le certificat de qualification si celle-ci ne dispose plus de certificat de qualification ou ne remplit plus les conditions requises par l'avant-projet de loi ?

En l'absence de précisions des auteurs de l'avant-projet de loi quant aux critères qui justifieraient une telle durée, la Commission nationale n'est pas en mesure d'apprécier si, en l'occurrence, le principe de durée de conservation limitée des données est respecté concernant la collecte de ces données.

En outre, il y a lieu de préciser qu'une durée de conservation devrait également être déterminée pour chaque catégorie de données à caractère personnel qui seraient collectées par le ministre dans le cadre de l'avant-projet de loi sous avis. A titre d'exemple, les données collectées lors de la procédure de délivrance des certificats de qualification de l'Union devront être supprimées ou anonymisées dès que leur conservation n'est plus nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Dès lors, même si la durée de conservation ne doit pas forcément être définie dans l'avant-projet de loi, celui-ci devrait a minima préciser les critères qui seraient pris en compte afin de déterminer quelle est la durée de conservation proportionnée pour chaque catégorie de données à caractère personnel qui serait collectée par le ministre.

II. Sur les échanges de données à caractère personnel

L'article 23 paragraphe (2) prévoit notamment que *« [l]e ministre échange des informations pertinentes avec les autorités compétentes des autres États membres concernant la certification des personnes intervenant dans l'exploitation d'un bâtiment, y compris les informations relatives à la suspension et au retrait des certificats »*.

Il convient de rappeler que les données à caractère personnel peuvent, en principe, circuler librement depuis le Grand-Duché de Luxembourg au sein de l'Espace économique européen, tant que les principes généraux du RGPD sont respectés. Il faudra notamment veiller à respecter le principe de la limitation des finalités, en vertu duquel les données ne doivent pas être traitées pour des finalités « incompatibles » avec les finalités d'origine.

En outre et dans la mesure où les modalités de ces échanges de données sont prévues par le règlement délégué (UE) 2020/473 de la Commission du 20 janvier 2020 en ce qui concerne les normes applicables aux bases de données relatives aux certificats de qualification de l'Union, aux livrets de service et aux livres de bord, cet article ne soulève pas d'observations de la part de la CNPD.

Ainsi décidé à Belvaux en date du 17 décembre 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

ANNEXES

5

Avis relatif au projet de loi n°7738 modifiant : 1° la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 ; 2° la loi du 19 décembre 2020 ayant pour objet la mise en place d'une contribution temporaire de l'État aux coûts non couverts de certaines entreprises ; 3° la loi modifiée du 4 juillet 2008 sur la jeunesse.

(Délibération n°30/2020 du 22 décembre 2020)

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 ».*

En date du 21 décembre 2020, Madame la Ministre de la Santé a saisi la Commission nationale d'une demande d'avis sur le projet de loi n°7738 modifiant : 1° la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 ; 2° la loi du 19 décembre 2020 ayant pour objet la mise en place d'une contribution temporaire de l'État aux coûts non couverts de certaines entreprises ; 3° la loi modifiée du 4 juillet 2008 sur la jeunesse (ci-après le « projet de loi n°7738 »).

Le présent projet de loi a pour objet de s'assurer que le système de santé national puisse continuer à fonctionner de manière adéquate dans l'intérêt de tous les patients et que le nombre des infections au virus SARS-CoV-2 puisse diminuer de manière significative. Il est dès lors proposé de maintenir certaines mesures de lutte contre la pandémie Covid-19 déjà en place, d'en renforcer d'autres et d'en prendre de nouvelles qui s'appliqueront pendant la période du 26 décembre 2020 au 10 janvier 2021.

La CNPD tient à souligner que vu l'urgence du projet de loi sous avis, il ne lui est pas possible d'analyser en profondeur les modifications proposées et que son avis a été élaboré et adopté uniquement sur base des informations dont elle dispose à ce jour. L'avis est rendu sous réserve d'éventuelles considérations futures.

1. Ad article 9 du projet de loi n°7738

L'article 9 du projet de loi n°7738 vise à modifier l'article 5 paragraphe (3) de la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 en précisant que la transmission par les professionnels de santé au directeur de la santé de certaines données à caractère personnel des personnes dont le résultat d'un test diagnostique de l'infection au virus SARS-CoV-2 a été négatif a pour but non seulement de suivre l'évolution de la propagation du virus, mais aussi d'acquérir les connaissances fondamentales relatives à cette évolution.

Par ailleurs, selon l'article 5 paragraphe (3) point 2 nouveau de la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19, les laboratoires d'analyses médicales sont obligés de transmettre au directeur de la santé les nom, prénoms, sexe, numéro d'identification ou date de naissance, la commune de résidence ou l'adresse des personnes qui se sont soumises à un test sérologique, ainsi que le résultat de ce test. Ces données sont anonymisées par le directeur de la santé ou son délégué à l'issue d'une durée de deux ans. D'après l'exposé des motifs, comme *« le taux d'anticorps contre le SARS-CoV-2 décroit avec le temps, cette signature immunitaire de l'infection n'a de valeur que pendant une durée limitée. Pour cette raison, la durée de conservation la plus appropriée s'avère être de deux ans. »*

A ce titre, la Commission nationale renvoie au point 2.3 du présent avis, et ce sous réserve de considérations futures de sa part.

2. Ad article 10 du projet de loi n°7738 : la collecte des données à caractère personnel dans le cadre du programme de vaccination

2.1. Remarques préliminaires

En ce qui concerne la base légale sur laquelle repose a priori le traitement opéré par directeur de la santé en vue de suivre l'évolution de la propagation du virus SARS-CoV-2, plus précisément l'intérêt public en vertu de l'article 6 paragraphe (1) lettre e) tout comme l'article 9 paragraphe 2) lettre i) du RGPD, la CNPD tient à renvoyer à ses commentaires y relatifs dans son avis initial relatif au projet de loi n°7606 portant introduction d'une série de mesures concernant les personnes physiques dans le cadre de la lutte contre le virus SARS-CoV-2 (COVID-19).[178]

Néanmoins, elle tient à préciser que l'article 6 paragraphe (3) du RGPD 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 définis soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis.

[178] Délibération n°13/2020 du 8 juin 2020.

De plus, 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. […] ».* Le considérant 41 du RGPD précise encore que 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 et de la Cour européenne des droits de l'homme.

Ainsi, s'il ne faut pas qu'un texte normatif national ou supranational prescrive spécifiquement un traitement de données, *« la finalité du traitement doit cependant être précise, dans la mesure où le texte amenant l'administration à traiter des données doit permettre aux administrés d'en déduire la nature des données et les fins pour lesquelles celles-ci sont utilisées »*[179].

2.2. Quant à la finalité poursuivie par la collecte des données dans le cadre du programme de vaccination

L'article 10 paragraphe (1) nouveau de la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 prévoit que le système d'information mis en place par le directeur de la santé en vue de suivre l'évolution de la propagation du virus SARS-CoV-2 poursuit dorénavant une finalité supplémentaire : *« suivre et évaluer de manière continue l'efficacité et la sécurité des vaccins contre la Covid-19. »*

En vertu de l'article 10 point 2° du projet de loi n°7738, le nouveau point 3 de l'article 10 paragraphe (2) de la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 prévoit ainsi que le système d'information mis en place par le directeur de la santé porte, en sus des données initialement y contenues,[180] sur toute une série de données à caractère personnel collectées dans le cadre du programme de vaccination concernant le vaccinateur, d'une part, c'est-à-dire le médecin en charge de poser ou de confirmer l'indication de la vaccination et de prescrire le vaccin afin de mettre en place ce système de surveillance,[181] ainsi que la personne à vacciner, d'autre part.

Néanmoins, sur base des éléments dont elle dispose à l'heure actuelle, la Commission nationale a des difficultés à saisir la finalité précise de la collecte et de l'enregistrement au système d'information de toutes ces données à caractère personnel concernant le vaccinateur et la personne à vacciner. L'article 5 paragraphe (1) lettre (b) du RGPD exige en effet que 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 ».*

L'exposé des motifs est assez vague à cet égard en précisant uniquement qu'il convient *« d'assurer un suivi spécifique de la qualité et des effets des différents vaccins notamment afin de renforcer la confiance de la population envers la vaccination »* et que ce *« suivi inclut également les activités usuelles de mesure de la couverture vaccinale, de mesure de l'efficacité des vaccins et de pharmacovigilance. […] En effet, il s'avère nécessaire de vérifier l'utilité réelle de la vaccination en vue d'en identifier les bénéfices. Enfin, ce suivi permettra d'ajuster la stratégie vaccinale et le plan de déploiement. »*

[179] M. Besch, « Traitement de données à caractère personnel dans le secteur public », Normes et légistique en droit public luxembourgeois, Luxembourg, Promoculture Larcier, 2019, p.470, n°619

[180] Il s'agit des données collectées en vertu de l'article 5 de la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19 et des données collectées en vertu des articles 3 à 5 de la loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique.

[181] Comme précisé dans le commentaire de l'article 10 du projet de loi sous avis.

Considérant les déclarations du gouvernement que la vaccination contre le coronavirus ne sera pas obligatoire, la CNPD se demande ainsi en quoi consiste exactement la finalité poursuivie par le traitement des données à caractère personnel du vaccinateur et de la personne à vacciner. La finalité telle qu'indiquée, s'inscrit-elle ou est-elle limitée dans un contexte de pharmacovigilance[182] ou d'exigences de loi du 4 juillet 2000 relative à la responsabilité de l'État en matière de vaccinations consacrant la responsabilité de l'État dans certains cas de séquelles dues à une vaccination légale réglementaire ou recommandée par l'État ?

Vu l'urgence et le manque de précision dans le commentaire des articles, la CNPD n'a pas été en mesure de rechercher et d'analyser les textes légaux en la matière. Elle s'interroge dès lors également si des données similaires sont collectées et enregistrées dans des fichiers étatiques dans le cadre de vaccinations contre d'autres maladies ou pathologies, notamment celles énumérées au règlement grand-ducal modifié du 18 octobre 2001 déterminant la liste des vaccinations recommandées.

Enfin, la Commission nationale se demande dans ce contexte si les auteurs du projet de loi ne font pas, par ailleurs, implicitement référence à un traitement ultérieur des données collectées dans un but de recherche scientifique ?

Afin de répondre aux exigences de prévision et de prévisibilité auxquelles doit répondre un texte légal, par référence à la jurisprudence européenne, et dans un souci de transparence et de sécurité juridique, la CNPD recommande aux auteurs du projet de loi de préciser dans le corps du texte de manière plus détaillée quelles sont les finalités explicites et déterminées réellement poursuivies par la collecte de ce nombre élevé de données à caractère personnel concernant le vaccinateur et la personne à vacciner.

2.3. Concernant la durée de conservation des données collectées dans le cadre du programme de vaccination

L'article 5 paragraphe (1) lettre (e) du RGPD prévoit que 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 »*. Il ressort par ailleurs du considérant (45) du RGPD que lorsque 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, il devrait appartenir au droit de l'Union ou au droit d'un État membre d'établir, entre autres, la durée de conservation des données.

Ainsi, la durée de conservation doit être déterminée en fonction de l'objectif ayant conduit à la collecte des données en cause. Une fois cet objectif atteint, ces données devraient être supprimées ou anonymisées (afin notamment de produire des statistiques).

Le point 4° de l'article 10 du projet de loi n°7738 prévoit dans ce contexte que les données à caractère personnel des vaccinateurs sont anonymisées au plus tard à l'issue d'une durée de deux ans après leur collecte, tandis que

[182] Comme prévu par l'article 4 paragraphe (5) de la loi modifiée du 21 novembre 1980 portant organisation de la Direction de la santé et la loi modifiée du 16 août 1968 portant création d'un Centre de logopédie et de services audiométrique et orthophonique.

les données à caractère personnel des personnes à vacciner sont anonymisées au plus tard à l'issue d'une durée de vingt ans après leur collecte.

L'exposé des motifs précise dans ce contexte que *« les données des personnes vaccinées seront conservées pendant vingt ans à compter de la date de collecte, période minimale permettant d'assurer le suivi optimal de la vaccination, dans une optique de protection des personnes vaccinées sur le long terme. En effet, il ne faut pas oublier que nous sommes en présence d'un vaccin nouveau qui est déployé et dont les effets se manifesteront en temps réels. Il est dès lors dans l'intérêt même de la personne vaccinée que les données la concernant soient conservées le plus longtemps possible afin de vérifier si un effet apparaissant au bout de plusieurs années peut, le cas échéant, être mis en relation avec le vaccin ou non. En revanche, s'agissant des données des vaccinateurs, celles-ci seront conservées pendant deux ans. Ceci s'explique par leur nécessité en vue d'assurer le suivi des effets indésirables sur les courts et moyens termes uniquement. Cette collecte ayant un autre objectif, le principe de proportionnalité commande des délais de conservation plus courts. »*

Au regard du RGPD, il est nécessaire et primordial de définir une durée de conservation des données au sein du système d'information de la direction de la santé qui soit proportionnée au regard de la finalité poursuivie. Partant, il est nécessaire de définir des critères objectifs permettant de justifier une durée de conservation adéquate.

Néanmoins, la Commission nationale ne dispose pas de l'expertise scientifique et épidémiologique nécessaire, afin d'évaluer si la conservation des données des personnes vaccinées pendant vingt ans à compter de la date de collecte est vraiment nécessaire et proportionné, au regard de la finalité vague et imprécise telle qu'indiquée dans le texte du projet de loi.

La CNPD saisit l'occasion pour souligner l'importance fondamentale du droit à l'information des personnes concernées. En vertu des articles 13 et 14 du RGPD, le responsable du traitement est en effet obligé de fournir aux personnes concernées certaines informations lorsque des données à caractère personnel sont collectées directement auprès d'elles ou indirectement à travers un tiers. Une information précise et adaptée devra donc être apportée aux personnes concernées dans un contexte sanitaire particulier, tant aux vaccinateurs et surtout aux personnes à vacciner, en particulier de toute utilisation ultérieure de leurs données, ayant à l'esprit que le délai de conservation des données prévu est de vingt ans.

Finalement, faute de précision dans le texte du projet de loi n°7738, la CNPD se demande quelle est l'origine des données à caractère personnel des vaccinateurs et des personnes vaccinées, c'est-à-dire qui est obligé de collecter, ainsi que de transmettre et d'enregistrer les données en cause dans le système d'information de la direction de la santé. S'agit-il des vaccinateurs-mêmes qui sont en charge du programme de vaccination dans les centres de vaccinations ?[183] Ou est-ce qu'à court et moyen terme il est aussi prévu que les médecins référents peuvent directement vacciner leurs patients et dans ce cas, ils seraient obligés de transmettre les données en cause à

[183] A voir dans ce contexte la stratégie de vaccination contre la COVID-19 du Luxembourg : https://sante.public.lu/fr/actualites/2020/12/communique-strategie-vaccination/index.html.

la direction de la santé ? En outre, il y a lieu de s'interroger qu'est-ce qu'il advient des données ainsi collectées par les vaccinateurs et transmises ensuite à la direction de la santé. Est-ce que les données collectées par les vaccinateurs sont-elles immédiatement détruites dès la transmission ou restent-elles enregistrées dans des fichiers des vaccinateurs pendant un certain délai ?

Ces points mériteraient d'être clarifiés et précisés dans le texte du projet de loi.

Ainsi décidé à Belvaux en date du 22 décembre 2020.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann
Présidente	Commissaire	Commissaire

ANNEXES

5

Avis relatif au projet de loi 7652 modifiant : 1° la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés ; 2° la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques.

(Délibération n°32/2020 du 30 décembre 2020)

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 ».*

Par courrier en date du 21 juillet 2020, Monsieur le Ministre de la Mobilité et des Travaux publics a informé la Commission nationale de l'élaboration d'un avant-projet de loi afin d'adapter le cadre légal de la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés (ci-après désignée « la loi modifiée du 25 juillet 2015 ») en vue de la mise en place de « radars feux rouges ». En date du 20 août 2020, le projet de loi 7652 modifiant 1° la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés et 2° la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques, a été déposé à la Chambre des Députés.

N'ayant pas été directement saisie par Monsieur le Ministre, ni au stade de l'avant-projet, ni au stade du projet de loi, la CNPD souhaite néanmoins se prononcer quant au projet loi 7652, et quant aux interactions de ce dernier avec le cadre légal relatif à la protection des données à caractère personnel. Cette autosaisie s'explique par le fait que la Commission nationale s'était d'ores et déjà prononcée quant au projet de loi portant création du système de contrôle et de sanction automatisé et portant modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques[184].

Le projet de loi sous avis s'intègre dans le plan d'action « sécurité routière » (2019-2023) adopté par le Gouvernement comprenant diverses mesures à mettre en œuvre d'ici 2023 afin de lutter contre les accidents de la route et d'améliorer la sécurité routière. À cet égard, l'exposé des motifs du projet de loi explique que *« la mesure 14 de ce plan d'action prévoit le renforcement du respect des feux rouges notamment par le biais d'installation de « radars feux rouges ». Ces radars sont conçus pour détecter le non-respect d'un signal lumineux rouge de façon systématique et automatique ».*

[184] Avis de la Commission nationale pour la protection des données du 25 février 2015 (document parlementaire 6714/05).

Outre l'excès de vitesse, comme c'est déjà le cas, et l'inobservation d'un feu rouge, tel qu'expliqué ci-dessus, la finalité du système CSA, à plus long terme, est également de constater deux autres types d'infractions au Code de la route, à savoir le non-respect des distances de sécurité entre les véhicules, et le fait de circuler sur des voies réservées à d'autres usagers de la route.

Dans ce contexte, il est proposé d'adapter le cadre légal pour les radars automatiques fixé par la loi modifiée du 25 juillet 2015 en vue de la mise en place de radars destinés à constater ces types d'infractions.

À cet égard, la CNPD tient à faire part de ses observations par rapport à certaines dispositions du projet de loi présentant des aspects ayant trait à la protection des données à caractère personnel, en ce qui concerne en particulier la mise en place de radars de type « feux rouges ».

I. <u>Observations générales quant au cadre légal</u>

À titre liminaire la CNPD note que le projet de loi propose de modifier l'article 3 alinéa 2 paragraphe 1er de la loi modifiée du 25 juillet 2015 en prévoyant un élargissement de la prise en compte des infractions au Code de la route par les radars automatiques. Si ces derniers ne constatent pour l'heure que le non-respect des limitations de vitesses, ils seront en outre amenés à mesurer : *« 1. La vitesse des véhicules en rapprochement ou en éloignement, 2. La vitesse moyenne des véhicules entre deux points, 3. L'inobservation d'un signal lumineux rouge, 4. La distance par rapport au véhicule qui précède correspondant à un temps de parcours d'au moins deux secondes, 5. Le fait de circuler sur une bande d'arrêt d'urgence, une partie de la chaussée réservée à d'autres usagers ou une voie fermée. ».*

La CNPD salue le choix du gouvernement de doter d'une base légale l'installation des radars automatiques ayant l'ensemble de ces fonctionnalités. Elle constate qu'une telle démarche a également eu lieu dans bon nombre de pays européens. À titre d'exemple, ces dernières années, la France[185] et la Belgique[186] ont procédé à l'installation de radars feux rouges aux abords de leurs routes et élaboré un cadre légal en ce sens. Les finalités de l'installation des radars feux rouge dans ces pays sont communes à celles du Luxembourg puisqu'elles tendent également à faire diminuer le sentiment d'impunité du conducteur et renforcer la sécurité routière. Les radars feux rouges y sont généralement installés dans des milieux urbains denses afin d'assurer la protection des usagers dans des lieux fréquentés par les piétons, dans les cas où l'action de traverser la route est particulièrement dangereuse mais aussi et surtout dans des axes très fréquentés.

II. <u>Quant aux images prises par les radars feux rouges</u>

La CNPD observe que lors de la constatation de l'inobservation d'un signal lumineux rouge, en fonction de l'endroit où il est installé et de l'angle de la caméra, un radar serait susceptible non seulement de capturer la

[185] En ce sens, voir l'Arrêté du 13 octobre 2004 portant création du système de contrôle automatisé. Au 1er juillet 2017 701 radars feux rouges étaient d'ores et déjà déployés. Ces chiffres peuvent être retrouvés à la page https://www.securite-routiere.gouv.fr/radars/differents-types-de-radars/radars-fixes/radars-de-franchissement, consultée pour la dernière fois le 18/11/2020.

[186] En ce sens, voir l'Arrêté royal du 12 octobre 2010 relatif à l'approbation, à la vérification et à l'installation des instruments de mesure. Belgique, la 6ème réforme de l'État par rapport aux équipements routiers liés à la sécurité routière a doté les régions de compétences relatives au franchissement des feux rouges et d'équiper ces derniers de radars. Ainsi en Flandre, l'Arrêté du gouvernement flamand du 10 juillet 2015 et en Wallonie, l'Arrêté du Gouvernement wallon du 21 juin 2018 viennent modifier l'Arrêté royal du 12 octobre 2010 précédemment mentionné.

plaque d'immatriculation du véhicule, la photo du conducteur, du passager, mais également celles des personnes physiques circulant sur la voie publique, tels que des piétons traversant la route à cette endroit. En fonction de la configuration des lieux et du degré de fréquentation de l'espace public, un radar pourrait donc capturer les images des visages autres que celles des personnes présentes dans le véhicule.

Il est vrai que l'article 11, paragraphe (3) de la loi modifiée du 25 juillet 2015 prévoit que « *lors de l'exercice du droit d'accès, toute personne autre que le conducteur est masquée sur la photo exhibée, sauf si la photo concerne un véhicule utilisé au moment de l'infraction dans le cadre de l'apprentissage ou de l'examen pratiques en vue de l'obtention du permis de conduire* ». Cet article ne mentionne toutefois pas la présence de personnes tierces sur les images prises par les radars, tels que d'éventuels piétons.

La CNPD estime dès lors nécessaire de masquer automatiquement les images des piétons et de toute personne autre que le conducteur, qui n'auraient aucun lien avec l'infraction. En outre, la CNPD réitère ses interrogations, déjà exprimées dans son avis quant au projet de loi portant création du système de contrôle et de sanction automatisé et modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques[187], quant à la pertinence de se limiter aux masquages des personnes tierces à l'infraction uniquement lors de l'exercice du droit d'accès aux images du conducteur ou de la personne présumée pécuniairement responsable.

Elle estime également nécessaire d'envisager un masquage automatique des personnes physiques aux abords des routes qui sont prises lors de la capture d'image, et un masquage temporaire des passagers du véhicule afin que ces derniers puissent être à nouveau rendus visibles à l'occasion d'une éventuelle procédure judiciaire. Un tel mécanisme paraîtrait en effet davantage conforme au principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre (c) du RGPD, qui prévoit que les données à caractère personnelles doivent être « *(…) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (…)* ».

III. <u>Quant à l'information du public de l'existence des radars feux rouges</u>

La Commission nationale constate que le projet de loi ne fait pas état de l'information du public de l'existence de ces radars aux feux rouges. La CNPD rappelle que l'article 12 paragraphe 1 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 que matière de sécurité intérieure prévoit un minimum d'informations devant être fournies aux personnes concernées. Cet article dispose que « *Le responsable du traitement met à la disposition de la personne concernée au moins les informations suivantes :*

a) L'identité et les coordonnées du responsable du traitement ;
b) Les coordonnées du délégué à la protection des données ;

[187] Avis de la Commission nationale pour la protection des données du 25 février 2015 (document parlementaire 6714/05), p. 4.

c) Les finalités du traitement auquel sont destinées les données à caractère personnel ;
d) Le droit d'introduire une réclamation auprès d'une des deux autorités de contrôle visées aux articles 39 et 40 et les coordonnées de ladite autorité ;
e) L'existence du droit de demander au responsable du traitement des données à caractère personnel relatives à une personne concernée ».

Le paragraphe (3) du même article prévoit toutefois que *« le responsable du traitement peut retarder ou limiter la fourniture des informations à la personne concernée en application du paragraphe 2, ou ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, eu égard à la finalité du traitement concerné, et en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée, pour :*

a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ;
b) éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ;
c) protéger la sécurité publique ;
d) protéger la sécurité nationale et la défense nationale ; ou
e) protéger les droits et libertés d'autrui ».

Etant donné que l'installation de radars automatiques aux feux rouges concerne un public beaucoup plus large dépassant simplement les conducteurs et les passagers se trouvant à bord de véhicules, la CNPD entend attirer l'attention des auteurs du projet de loi sur l'obligation d'information de l'ensemble des personnes concernées de l'existence de ces radars et du traitement de données les concernant (p.ex. panneaux informant les conducteurs et passagers de véhicules ainsi que piétons aux endroits des radars installés aux feux rouges). S'il est envisagé de limiter ou de retarder cette information, il faudrait que la Police grand-ducale puisse justifier cette limitation ou retardement du droit à l'information par l'une des hypothèses visées à l'article 12 paragraphe (3) cité ci-dessus, voire le préciser dans le texte du projet de loi sous examen.

IV. Quant à la phase test de l'installation des radars feux rouges

La Commission nationale comprend qu'un premier radar feu rouge est installé dans un lieu très fréquenté de Luxembourg-Ville, Place de l'Etoile pour une phase de test[188]. Le ministre de la Mobilité et des Travaux publics annonce également l'installation effective dudit radar vers décembre 2020/janvier 2021 ainsi que l'installation supplémentaire de 2 radars feux rouges à Hollerich et au Schlammestee au cours de l'année 2021[189]. Dans ce contexte, la Commission nationale considère qu'il est opportun de profiter de la phase test afin d'observer si l'installation de ces radars feux rouges pose question en termes de protection des données (comme évoqué ci-dessus : des piétons apparaissent-ils sur les images ? les personnes concernées sont-elles correctement informées

[188] RTL, 5 minutes, « Le premier radar feu rouge du pays est en cours d'installation », article du 07/10/2020 disponible à la page, https://5minutes.rtl.lu/actu/luxembourg/a/1591684.html, consultée pour la dernière fois le 09/12/2020.
[189] Communiqué de presse du gouvernement luxembourgeois du 08/06/2020, "Mise en service en service du premier radar-tronçon dans le cadre de la lutte contre l'insécurité routière », communiqué disponible à la page https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2020/06-juin/08-bausch-radar.html, consultée pour la dernière fois le 09/12/2020.

de la présence de tels radars, comme développé à la section 4 ci-dessus ? certaines d'entre elles ont-elles été amenées à exercer leur droit d'accès (y compris pour obtenir copie de l'image prise par le radar) ? avec quel résultat ? etc.). Ce retour d'expériences peut être particulièrement bénéfique et apporter des éléments de réponses aux interrogations soulevées dans le présent avis.

V. <u>Quant à l'exercice du droit d'accès aux données du système CSA par les personnes concernées</u>

En ce qui concerne le droit d'accès aux données du système CSA, la CNPD constate que le législateur n'a pas tenu compte de sa position exprimée dans son avis précédemment mentionné[190]. En effet, l'article 11 paragraphe 1 de la loi modifiée du 25 juillet 2015 prévoit : « […] le droit de consulter la photo concernant le véhicule en infraction et les données à caractère personnel la concernant traitées dans le cadre de l'exploitation du système CSA ». L'article 11 paragraphe 2 dispose que : « Cette consultation se fait au Centre et sous le contrôle de la Police grand-ducale ». À cet égard, la Commission nationale se demande à nouveau si l'obligation pour la personne pécuniairement responsable ou la personne désignée comme conducteur du véhicule au moment de l'infraction de se déplacer au Centre se trouvant à Bertrange, ne constitue pas un obstacle injustifié au droit d'accès de cette personne ?

Or, cette problématique se pose d'autant plus suite à l'entrée en application 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, dont l'article 11 prévoit dans ses paragraphes (1) et (2) que :

« (1) Le responsable du traitement prend des mesures raisonnables pour fournir toute information visée à l'article 12 et procède à toute communication relative au traitement ayant trait à l'article 10, aux articles 13 à 17 et à l'article 30 à la personne concernée d'une façon concise, compréhensible et aisément accessible, en des termes clairs et simples. Les informations sont fournies par tout moyen approprié, y compris par voie électronique. De manière générale, le responsable du traitement fournit les informations sous la même forme que la demande.

(2) Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée par l'article 10 et les articles 13 à 17. ».

L'article 13 de la loi précitée prévoit quant à lui que :

« Sous réserve de l'article 14, la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données ainsi que les informations suivantes :

a) les finalités du traitement ainsi que sa base juridique ;

[190] Avis de la Commission nationale pour la protection des données du 25 février 2015 (document parlementaire 6714/05), p. 4.

b) les catégories de données à caractère personnel concernées ;

c) les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales ;

d) lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

e) l'existence du droit de demander au responsable du traitement la rectification ou l'effacement des données à caractère personnel, ou la limitation du traitement des données à caractère personnel relatives à la personne concernée ;

f) le droit d'introduire une réclamation auprès de l'une des deux autorités de contrôle compétentes visées aux articles 39 et 40 et les coordonnées de ladite autorité ;

g) la communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible quant à leur source ».

Dans ce contexte, depuis l'entrée en application de la loi modifiée du 25 juillet 2015, la Commission nationale a été saisie de nombreuses demandes d'informations et de réclamations, de citoyens s'interrogeant sur la nécessité de devoir se déplacer au Centre à Bertrange afin de consulter la photo concernant le véhicule en infraction, et ainsi d'exercer leur droit d'accès, ce qui pose effectivement la question de la compatibilité de l'article 11 de cette loi avec la loi précitée du 1er août 2018.

Il y a encore lieu de relever à cet égard la pétition publique n°1216 « pour l'obtention/l'envoi d'une copie de la photo prise lors d'un contrôle automatisé (Radar) en matière de circulation », même s'il est vrai que cette pétition n'a pas obtenu le nombre de signatures requises afin de faire l'objet d'un débat public.

Par conséquent, la Commission nationale réitère sa position exprimée dans l'avis quant au projet de loi portant création du système de contrôle et de sanction automatisé et modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques. Dès lors, elle estime nécessaire de modifier l'article 11 paragraphe 2 de la loi modifiée du 25 juillet 2015 dans le but de permettre « […] à la personne pécuniairement responsable ou la personne désignée comme conducteur du véhicule au moment de l'infraction de consulter la photo concernant son véhicule, selon son choix, sur place au Centre, ou de recevoir communication de la photo via une demande écrite préalable adressée au Centre ».

VI. <u>Quant à la durée de conservation des photos</u>

La Commission nationale se demande si, à l'occasion de l'introduction du projet de loi 7652, il ne serait pas utile de clarifier la question de la durée de conservation des photos provenant des radars, qu'elle avait déjà soulevé dans son avis du 25 février 2015[191] ?

Les durées de conservation des données enregistrées sont actuellement prévues par l'article 4 du règlement grand-ducal du 7 août 2015 autorisant la création d'un fichier et le traitement de données à caractère personnel dans le cadre du système de contrôle et de sanction automatisé[192].

Par ailleurs, l'article 2 de ce même règlement grand-ducal indique que le fichier contient seulement les données « par infraction constatée et enregistrée ». Faut-il comprendre *a contrario* que s'il n'y a pas d'infraction constatée, les photos ne sont pas enregistrées et automatiquement détruites ?

Dans le cas contraire, il serait indispensable de prévoir dans la loi ou le règlement grand-ducal ce qu'il advient des images provenant des radars, alors qu'aux yeux de la CNPD, celles-ci devraient être immédiatement détruites dans l'hypothèse où aucune infraction ne serait constatée, afin de respecter le principe de la durée de conservation limitée des données, prévu à l'article 3 paragraphe (1) lettre e) de la loi précitée du 1er août 2018.

Ainsi décidé à Belvaux en date du 30 décembre 2020.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Lemmer Commissaire

[191] Avis de la Commission nationale pour la protection des données du 25 février 2015 (document parlementaire 6714/05), p. 7.
[192] Notons que ce règlement grand-ducal fait toujours référence à la loi abrogée du 2 août 2002, ayant été adopté avant le changement législatif introduit par la loi précitée du 1er août 2018.

CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

15, Boulevard du Jazz - L-4370 Belvaux
Téléphone : +352 26 10 60-1 - Fax : +352 26 10 60-6099
www.cnpd.lu