



RAPPORT ANNUEL 2021



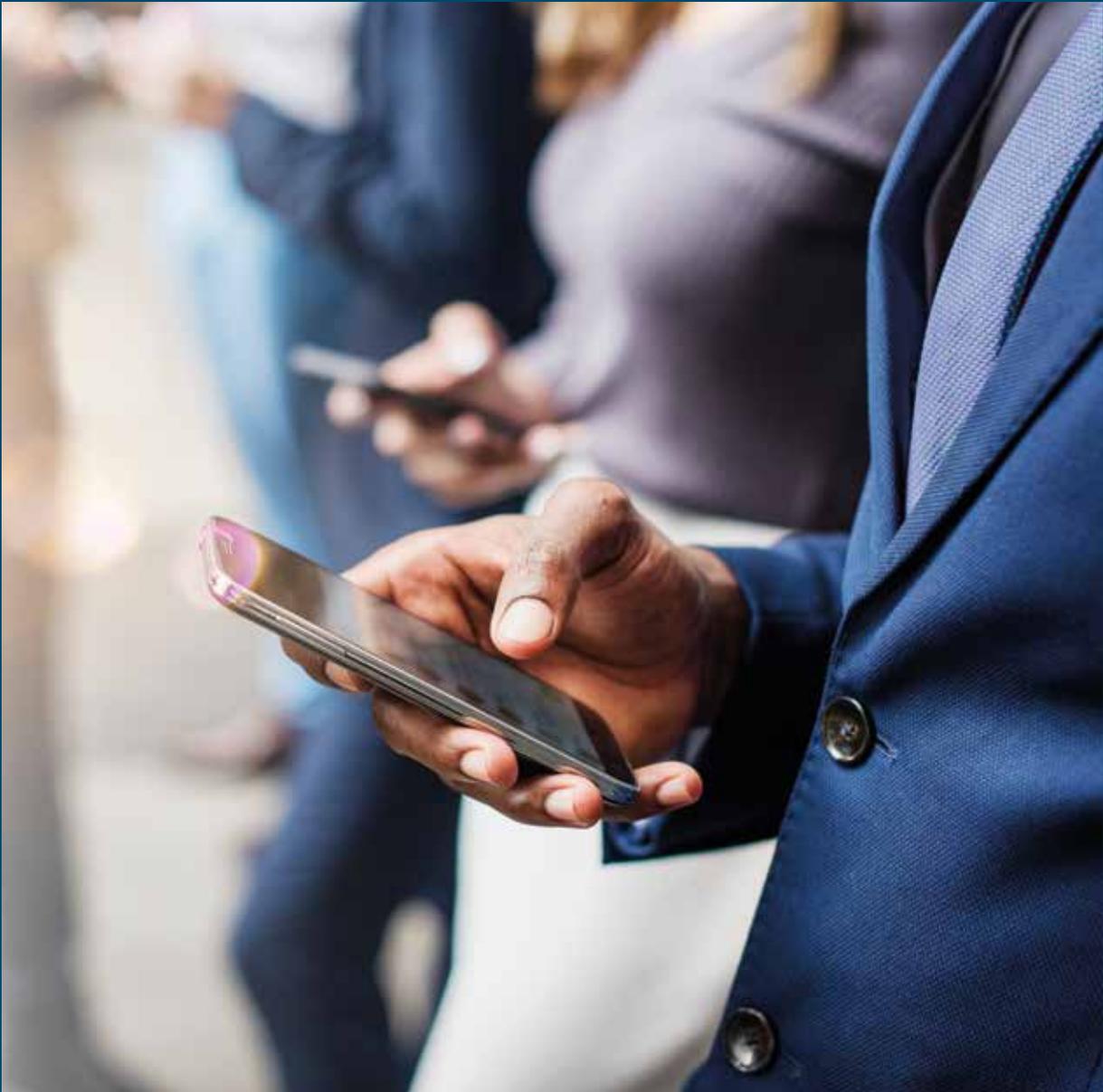


RAPPORT ANNUEL 2021



TABLE DES MATIÈRES

1 INTRODUCTION	P4	5 Contrôles prévus par des dispositions légales spécifiques	P80
2 AVANT-PROPOS	P10	6 Coopération européenne	P80
3 UNE ANNÉE EN CHIFFRES	P16	LA PROTECTION DE LA VIE PRIVÉE DANS LE SECTEUR DES COMMUNICATIONS ÉLECTRONIQUES	P83
4 LES ACTIVITÉS EN 2021	P26	1 Violations de données dans le secteur des communications électroniques	P83
LES ACTIVITÉS DANS LE CADRE DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES	P29	2 Rétention de données de trafic et de localisation	P84
1 Sensibiliser le public	P29	LES TRAVAUX INTERNATIONAUX DANS LE DOMAINE DE LA PROTECTION DES DONNÉES	P87
2 Répondre aux demandes d'information de particuliers et de professionnels	P36	1 European Data Protection Board (EDPB)	P88
3 Intervenir dans le processus législatif	P38	2 Conférence internationale de la Global Privacy Assembly (GPA)	P93
4 Guider les acteurs privés et publics	P44	3 Conférence de printemps des autorités européennes à la protection des données	P95
5 Désignation des délégués à la protection des données	P46	4 Le séminaire « European Case Handling Workshop »	P95
6 Accompagner la mise en conformité	P50	5 RESSOURCES, STRUCTURES ET FONCTIONNEMENT	P96
7 Traiter les réclamations des citoyens	P59	1 Ressources humaines	P98
8 Analyser les violations de données	P64	2 Organisation de la CNPD	P103
9 Contrôler et adopter des mesures correctrices	P69	3 Rapport de gestion relatif aux comptes de l'exercice 2021	P104
LE CONTRÔLE DES TRAITEMENTS DE DONNÉES DES AUTORITÉS RÉPRESSIVES OU DE SÉCURITÉ NATIONALE	P77	6 ANNEXES	P110
1 Demandes d'information	P77	Les annexes peuvent être téléchargées sur le site de la CNPD à l'adresse https://cnpd.public.lu/fr/publications/rapports/index.html	
2 Avis	P78		
3 Réclamations	P79		
4 Notification de violations de données	P79		



INTRODUCTION

1

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.

1

INTRODUCTION

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 1^{er} 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 1^{er} 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.

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.

1

INTRODUCTION

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.



LE COLLÈGE :
ALAIN HERRMANN, THIERRY LALLEMANG,
TINE A. LARSEN ET MARC LEMMER.



LE SIÈGE
DE LA CNPD
À BELVAL

AVANT-PROPOS

2



2

AVANT-PROPOS



TINE A. LARSEN
Présidente

« La CNPD, comme ses homologues européens au sein du EDPB, surveillent les technologies nouvelles et émergentes, ainsi que leur impact potentiel sur les droits fondamentaux et la vie quotidienne des citoyens. »

MADAME LARSEN, C'EST LE MOMENT DE FAIRE LE BILAN DE 2021. QUELS ONT ÉTÉ LES MOMENTS FORTS DE L'ANNÉE POUR LA CNPD ?

Tine A. Larsen : Plusieurs choses sont à mettre en exergue. D'abord, dans le contexte de la pandémie de Covid-19, nous avons assuré la continuité des affaires courantes dans le respect des protocoles sanitaires en vigueur : demandes de renseignements, réclamations nationales ou européennes... Malgré les difficultés liées à la pandémie, la CNPD a poursuivi ses missions. Nous avons aussi accueilli un nouveau commissaire en la personne de Monsieur Alain Hermann, en charge de la certification. Par ailleurs, les agents de la CNPD ont poursuivi leur engagement dans les divers sous-groupes du Comité européen pour la protection des données (EDPB). Mais surtout, nous avons publié nos premières décisions faisant suite aux enquêtes que nous avons ouvertes depuis l'entrée en vigueur du RGPD en 2018.

VOUS ÉVOQUEZ DES ENQUÊTES ET DES PRISES DE DÉCISIONS. POUVEZ-VOUS NOUS EN DIRE PLUS ?

Nos enquêtes ont principalement débuté dans le courant de 2020 et des prises de décisions ont été réalisées en 2021. Au total, ce ne sont pas moins de 49 dossiers qui ont été clôturés, avec ou sans mesures correctrices et/ou amendes. Dans le détail, 12 enquêtes ont été clôturées en l'absence de manquements retenus, mais 37 enquêtes ont abouti à des mesures correctrices, dont 25 avec des amendes. Au total, 48 décisions se rapportaient à des affaires nationales, avec un montant global de 319.500 euros d'amendes administratives (soit entre 1.000 et 150.000 euros d'amende

selon les dossiers). Nous avons aussi pris une décision dans le cadre de la coopération européenne à l'encontre d'Amazon, avec une amende administrative de 746 millions d'euros.

DANS LE CADRE DE CES ENQUÊTES, QUELLES ÉTAIENT LES PROBLÉMATIQUES ANALYSÉES PAR LA CNPD ?

La majorité des décisions (25 au total) ont été prises dans le cadre de la campagne d'enquête thématique sur la fonction de délégué à la protection des données. 20 décisions concernaient le traitement des données opéré via un système de télésurveillance et/ou un dispositif de géolocalisation. Enfin, 4 décisions portaient sur des thématiques diverses : violations de données à caractère personnel, utilisation illicite de la banque de données JU-CHA dans le cadre d'une procédure de recrutement d'un employé de l'Etat au sein de l'administration judiciaire...

LA COVID-19 A AUSSI MARQUÉ L'ANNÉE 2021 ET LE TRAVAIL DE LA CNPD. QU'EN EST-IL EXACTEMENT ?

La CNPD et l'ensemble de ses collaborateurs ont poursuivi leur travail tout au long de 2021, dans le respect des protocoles et mesures sanitaires. Nous avons notamment été amenés à fournir des réponses aux citoyens sur leurs droits par rapport aux conditions d'utilisation de leurs données personnelles, notamment de santé. Nous avons publié des recommandations pour orienter les professionnels dans la poursuite de leurs activités ; nous avons établi une liste de FAQ relatives à l'utilisation de l'application CovidCheck.lu... D'autre part, comme en 2020, nous avons conseillé le Gouvernement pour les projets de loi Covid-19 réussis.

2

AVANT-PROPOS

LA COVID-19 N'A PAS MONOPOLISÉ TOUTE L'ANNÉE 2021. SUR QUELS AUTRES GRANDS SUJETS LA CNPD A-T-ELLE ÉTÉ SOLLICITÉE ?

2021 a aussi été marquée par un retour de thématiques « classiques », surtout en lien avec la vidéosurveillance et la surveillance du lieu de travail. Les personnes concernées ont principalement sollicité des informations sur l'exercice de leurs droits, surtout le droit d'accès et le droit à l'effacement. Ce genre de demandes reste assez stable d'une année sur l'autre : environ 600 par an, depuis 3 ans.

VOUS AVEZ ÉMIS 33 AVIS SUR DES PROJETS DE LOI OU DE RÈGLEMENTS GRAND-DUCAUX, SOIT 9 DE PLUS QU'UN AN AUPARAVANT. QUELLES ÉTAIENT LES PRINCIPALES THÉMATIQUES ABORDÉES ?

Les thématiques pour lesquelles l'avis de la CNPD a été sollicité ont été très diverses. Cela va de la lutte contre la pandémie de Covid-19 jusqu'aux cartes de stationnement pour personnes handicapées en passant par VISUPOL (la vidéosurveillance à des fins policières), le contrôle de l'acquisition et de la détention d'armes, la connaissance de ses origines dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs... D'autres thématiques très variées ont aussi été abordées, pour lesquelles la CNPD a émis des avis : les données ouvertes et la réutilisation des informations du secteur public, le contrôle d'honorabilité, le code des communications électroniques à l'échelle européenne, le fichier central de la police grand-ducale, l'organisation des services de taxis, le recensement général de la population, des logements et des bâtiments, ou les régimes internes des centres pénitentiaires.

LE « EUROPEAN DATA PROTECTION BOARD » (EDPB) EST COMPOSÉ DE REPRÉSENTANTS DES AUTORITÉS NATIONALES CHARGÉES DE LA PROTECTION DES DONNÉES. LA CNPD EN FAIT BIEN ENTENDU PARTIE. COMMENT CELLE-CI CONTRIBUE-T-ELLE AU EDPB ?

À ce niveau-là aussi, 2021 a été une année chargée. La CNPD a participé à 200 réunions plénières et des autres groupes de travail. Parfois, comme rapporteur ou co-rapporteur, la CNPD s'est impliquée dans la rédaction de plusieurs projets de lignes directrices et a assuré un suivi régulier des dossiers traités au niveau du Comité et des groupes. Nous avons également assuré le suivi de nouvelles propositions législatives par la Commission européenne. Nous avons encore encouragé et facilité l'utilisation de l'ensemble des outils de coopération et de cohérence prévus par le RGPD en vue d'actions coordonnées et de la mise en œuvre d'une collaboration transfrontalière uniforme et efficace. Mais surtout, après avoir contribué à la mise en place de procédures pour l'adoption des critères d'agrément des organismes de certification, des critères de certification et d'un label européen pour la certification, la CNPD a été la première autorité à soumettre des critères de certification au EDPB pour avis.

LA CNPD VA BIENTÔT CÉLÉBRER SON 20^{ÈME} ANNIVERSAIRE. LES DÉFIS QUI S'ANNONCENT AU COURS DES ANNÉES À VENIR SEMBLENT NOMBREUX ET DIVERSIFIÉS. POUR LA CNPD, QUELS SONT LES PRINCIPAUX DÉFIS QUI SE PROFILENT POUR LES PÉRIODES À VENIR ?

L'un des défis majeurs est l'apparition et le développement rapide de nouvelles technologies telles que des techniques d'intelligence artificielle et d'algorithmes. Le problème est

que la législation n'évolue pas aussi vite que la technologie. Heureusement, le RGPD a été conçu pour être neutre technologiquement : il n'entrave pas les progrès technologiques actuels et futurs et il n'empêche pas l'utilisation d'une technologie spécifique. Un autre grand défi consiste en l'élaboration de nombreuses nouvelles initiatives européennes telles que l'Artificial Intelligence Act, le Data Governance Act (adopté en mai 2022), le Digital Services Act (adopté en juillet 2022), le Data Act ou le Digital Markets Act (également adopté en juillet 2022). Tout l'enjeu consiste à intégrer ces nouvelles initiatives dans la législation existante tout en maintenant un même niveau de protection des données. C'est un défi important ! Il faut cependant souligner que tous les textes cités seront applicables sans préjudice du règlement RGPD et des autres règles de l'UE en matière de protection des données à caractère personnel. Il sera nécessaire de garantir une mise en place cohérente de ces textes et d'assurer une bonne coordination entre les autorités nationales qui seront désignées par les membres de l'UE.

LE NOMBRE CROISSANT DE NOUVELLES RÉGLEMENTATIONS VOUS INQUIÈTE-T-IL ?

On peut effectivement s'inquiéter du nombre croissant de nouveaux règlements qui viennent encadrer les données et donc se greffer sur le RGPD qui reste toutefois la référence en termes de données personnelles. Le risque est de constater à un certain moment un affaiblissement du cadre du RGPD plutôt qu'un renforcement de ce dernier. Il est clair que l'adoption des nouveaux actes et l'application des textes exigeront un grand effort de coordination. Les autorités seront confrontées à de nouveaux défis d'ordre institutionnel, organisationnel et de ressources humaines. Il ne faut jamais perdre de vue que c'est

justement l'humain qui est au cœur de ce véritable tsunami de données et de réglementations du traitement de ces données. Pour cela, il ne faut pas plus de règles, mais de meilleures règles. L'UE a compris qu'on ne peut plus minimiser davantage les données, mais qu'il est essentiel d'avoir des règles et d'encadrer les grands acteurs. Nous verrons comment se dessine l'avenir, nous verrons aussi si les nouvelles règles sont conviviales et facilement applicables ou trop lourdes. Mais l'on sait déjà que la Commission européenne se dotera de plus de pouvoirs par rapport à une surveillance hétérogène au niveau national par les Etats membres. Et il est aussi déjà très clair que la nouvelle politique digitale de l'UE constitue une chance pour une meilleure protection des données personnelles.

LES DÉFIS À VENIR SONT DONC NOMBREUX. COMMENT COMPTEZ-VOUS Y FAIRE FACE ?

La CNPD, comme ses homologues européens au sein du EDPB, surveillent les technologies nouvelles et émergentes, ainsi que leur impact potentiel sur les droits fondamentaux et la vie quotidienne des citoyens. L'EDPB a déjà élaboré des guidances sur les récents développements technologiques et l'utilisation des données biométriques. Il a aussi développé des lignes directrices sur l'utilisation de la reconnaissance faciale, la blockchain et d'autres technologies dans son programme de travail pour les deux prochaines années. ■



UNE ANNÉE EN CHIFFRES

3



3

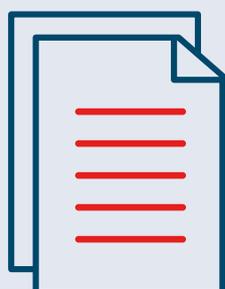
UNE ANNÉE EN CHIFFRES

Sensibilisation, guidance et conseil

33

AVIS

par rapport à 24 en 2020



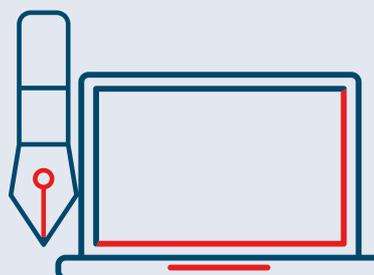
relatifs à des projets ou propositions de loi ou mesures réglementaires, dont notamment des avis sur les lois relatives :

- à la lutte contre la COVID-19 ;
- au système de vidéosurveillance à des fins policières « Visupol » ;
- aux données ouvertes et la réutilisation des informations du secteur public.

618

DEMANDES DE
RENSEIGNEMENT
PAR ÉCRIT

par rapport à 655 en 2020



Les 3 principales catégories de demandes concernent :

- la pandémie COVID-19 (traçage des personnes, prise de température, télétravail, homeschooling, etc.) ;
- la surveillance sur le lieu du travail ;
- le droit des personnes concernées (droit d'accès, droit d'effacement, etc.).

Sensibilisation, guidance et conseil

2

**NOUVELLES
GUIDANCES**



- Lignes directrices en matière de géolocalisation des véhicules mis à la disposition des salariés ;
- Lignes directrices en matière de cookies et autres traceurs.

13

**FORMATIONS
ET
CONFÉRENCES**

par rapport à 17 en 2020



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

3

UNE ANNÉE EN CHIFFRES

Conformité et contrôle

512

RÉCLAMATIONS

par rapport à 485 en 2020



Raisons principales :

1. Non-respect du droit d'accès (26 %) ;
2. Demande d'effacement ou de rectification non respectée (24 %) ;
3. Licéité du traitement (14 %).

333

NOTIFICATIONS DE VIOLATIONS DE DONNÉES

par rapport à 379 en 2020



Cause principale : erreur humaine (62 %).

Nature des incidents :

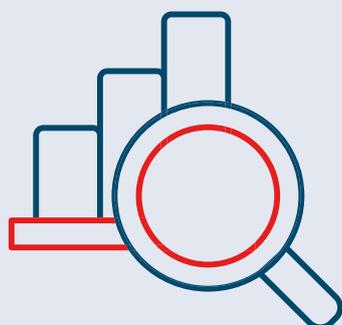
1. données personnelles envoyées au mauvais destinataire (30 %) ;
2. piratage, hacking (17 %) ;
3. divulgation des données personnelles à la mauvaise personne (12 %).

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

Conformité et contrôle

7

**AUDITS
OUVERTS**

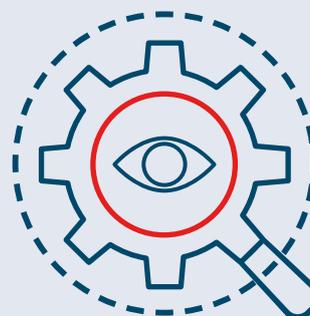


Dans le cadre de la campagne thématique « transparence » dans le secteur du commerce électronique et dans le cadre de la vérification de la conformité du système d'information mis en place dans le cadre de l'épidémie Covid.

18

**VISITES
SUR PLACE**

par rapport à 8 en 2020



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

3

UNE ANNÉE EN CHIFFRES

Décisions

49

DÉCISIONS PRISES
PAR LA FORMATION
RESTREINTE



- 12 clôturées en l'absence de manquements retenus
- 12 avec mesures correctrices
- 25 avec mesures correctrices et amendes

746 319 500 €

D'AMENDES
ADMINISTRATIVES



- 319 500 € dans des dossiers au niveau national ;
- 746 000 000 € dans des dossiers dans le cadre de la coopération européenne.

International EDPB (European Data Protection Board)

15

RÉUNIONS
PLÉNIÈRES



200

RÉUNIONS
DES GROUPES
DE TRAVAIL



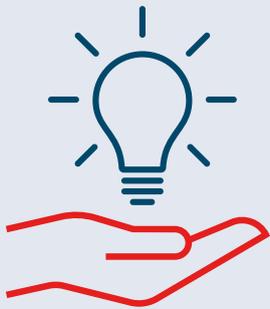
3

UNE ANNÉE EN CHIFFRES

International

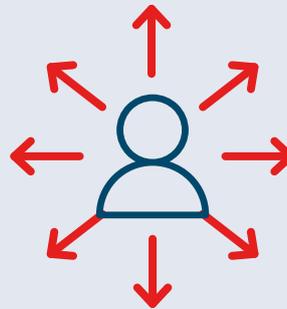
8

**NOUVELLES
LIGNES
DIRECTRICES**



6

PROJETS
pour lesquels la CNPD a
assumé le rôle de rapporteur
ou co-rapporteur

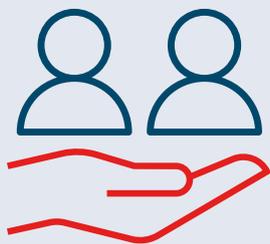


Ressources humaines

53

COLLABORATEURS

par rapport à 50 en 2020



37,5 ans : moyenne d'âge

4,5 ans : ancienneté moyenne





LES ACTIVITÉS EN 2021

4



4

LES ACTIVITÉS EN 2021



LES ACTIVITÉS DANS LE CADRE DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

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 leur faire connaître les droits et devoirs respectifs de chacun. Elle mène des actions de sensibilisation, informe le public à travers son site Internet en matière de protection des données personnelles et organise ou participe à des formations et conférences.

En raison de la pandémie, une partie des cours de formation traditionnellement organisés en présentiel a été transformée en cours à distance et d'autres parties ont été préenregistrés pour être diffusées sur des plateformes d'apprentissage.

28 JANVIER 2021 : 15^{ÈME} 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.

Conférence « Protection des données et de la vie privée face à la numérisation du travail »

Le 28 janvier 2021, la CNPD a organisé la conférence « Protection des données et de la vie privée face à la numérisation du travail » en mode virtuel.

Après l'allocation d'ouverture de la CNPD, M. Jean-Jacques Rommes, Président du CES (Conseil économique et social) a fait une présentation sur « L'impact des mutations technologiques sur le monde du travail » et Madame Isabelle Schlessler, Directrice de l'ADEM (Agence pour le développement de l'emploi) est intervenue sur le thème « Marché de l'emploi, digitalisation et données personnelles: enjeux pour l'ADEM ».

Les exposés ont été suivis par une table ronde animée par Monsieur Jürgen Stoldt.

Data Privacy Day

Dans le cadre de la Journée de la protection des données, la CNPD a également participé au Data Privacy Day, organisé par la Fondation

4

LES ACTIVITÉS EN 2021



Restena et l'Université du Luxembourg, avec une présentation intitulée « Updates from the CNPD: How COVID-19 shaped our work in 2020 ».

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.

ATELIERS DE TRAVAIL « DAPROLAB »

Les « DaProLab » (Data Protection Laboratory) sont des ateliers de travail proposés par la CNPD où un seul sujet spécifique défini à l'avance est discuté avec un nombre limité de personnes et sur lequel il y a un échange de connaissances, d'idées, d'interprétations et de points de vue.

La CNPD ne s'implique pas directement dans la discussion entre participants mais joue le rôle de modérateur de ces ateliers qui poursuivent l'objectif de développer la responsabilisation (accountability) parmi les responsables de traitement, principe phare du RGPD.

En 2021, la CNPD a organisé un seul DaProLab. Il s'agit d'un atelier de travail sollicité par le Service de Coordination de la Recherche et de l'Innovation Pédagogiques et Technologiques (SCRIPT), du Ministère de l'Education nationale, de l'Enfance et de la Jeunesse et ayant porté sur les registres de traitement de données.

FORMATIONS, CONFÉRENCES ET SÉMINAIRES

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

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

- « An introduction to GDPR for startups » dans le cadre du programme Fit 4 Start de Luxinnovat ;
- « The Power of Platforms and Markets », table ronde dans le cadre de la conférence RAID (Regulation of AI, Internet and Data) ;
- « La CNPD au coeur de la relation-client : Quelles règles à respecter à l'ère du digital ? », webinaire organisé par la Chambre des Métiers ;
- « La CNPD et les autorités de contrôle sous le RGPD », organisé par la Chambre des Salariés ;
- « RGPD : Comment le mettre en place dans mon bureau de courtage » organisé par l'APCAL (Association professionnelle des courtiers en assurances du Luxembourg) ;
- « Home, Sweet Home ? », table ronde dédiée à la problématique du télétravail dans le cadre des Luxembourg Internet Days organisés par LU-CIX ;
- « Quel bilan tirer un an après l'arrêt Schrems II sur les transferts internationaux de données ? » organisé par l'initiative HELP du Conseil de l'Europe en partenariat avec le Jeune Barreau de Luxembourg, la Commission immatérielle du Barreau de Luxembourg, l'Union internationale des avocats ;
- « The CNPD takes a stand » et « The latest news from the CNPD » lors des PwC Cybersecurity & Privacy Days 2021 ;
- « Fortbildungsseminar zur DSGVO: Untersuchungen in Bezug auf die Funktion des Datenschutzbeauftragten: Erkenntnisse der luxemburgischen Aufsichtsbehörde » organisé par la Private Universität im Fürstentum Liechtenstein ;
- « Introduction à la protection des données », organisé par l'ANELD (Association Nationale des Etudiants Luxembourgeois en Droit) ;
- Les Midis de l'Association luxembourgeoise des juristes de droit bancaire (ALJB).

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

4

LES ACTIVITÉS EN 2021

MARC LEMMER
Commissaire

« La sensibilisation
vise à valoriser
et à vulgariser le
travail de guidance
pour le rendre
compréhensible
par chacun »



MONSIEUR LEMMER, EN TANT QUE COMMISSAIRE, VOUS ÊTES NOTAMMENT EN CHARGE DE LA SENSIBILISATION. TOUT D'ABORD, POURQUOI LA CNPD INSISTE-ELLE SUR LA SENSIBILISATION ?

Marc Lemmer : La CNPD est une autorité de contrôle qui doit assurer un équilibre entre la sensibilisation des citoyens et des divers acteurs traitant des données personnelles, et la vérification de leurs activités par un travail d'enquête et, le cas échéant, la décision de mesures correctrices. La protection des données a été redéfinie en 2018 par le RGPD. Désormais, il y a moins de contrôles a priori, mais plus de responsabilisation des acteurs pour qu'ils respectent les réglementations en la matière. Il s'agit donc d'une approche sur la durée nécessitant un accompagnement de la gestion du changement.

QUELS SONT LES PUBLICS VISÉS PAR VOTRE TRAVAIL DE SENSIBILISATION ?

Il y a deux cibles principales. D'une part, les citoyens qui ont des droits par rapport à leurs données personnelles et au traitement de celles-ci. Ils doivent connaître ces droits, les règles en vigueur, les garanties qui leur sont données... D'autre part, il y a l'ensemble des responsables du traitement des données et leurs sous-traitants, aussi bien dans le secteur public que privé. La sensibilisation vise à mieux leur faire prendre conscience des réglementations et de leurs obligations en la matière.

COMMENT PROCÉDEZ-VOUS ?

Le travail de sensibilisation n'arrive pas en première ligne, mais fait suite à un travail en amont. Un travail de guidance mené entre autres par les juristes de la CNPD ou à l'échelle européenne. Ils élaborent les lignes directrices pour les différents acteurs. La sensibilisation vise à valoriser et à vulgariser le travail de guidance pour le rendre compréhensible par chacun : citoyens, organisations publiques (ministères, communes...), PME et grandes entreprises du privé, monde associatif ... Notre travail de sensibilisation suit 3 grands axes : la communication externe et la sensibilisation,

le développement de formations avec des acteurs de la formation continue ou via des formats développés par la CNPD, ainsi que des activités de prospective et de collaboration avec le monde de la recherche et de l'innovation dans le domaine de la protection des données, des nouvelles technologies comme par exemple l'intelligence artificielle...

DANS CE CONTEXTE, QUELLES ONT ÉTÉ VOS PLUS GRANDES ACTIONS EN 2021 ?

Malgré la pandémie de Covid-19 et les mesures sanitaires en vigueur, nous avons mené diverses actions, même si certains événements en présentiel ont dû être reportés et même si certaines ressources allouées à des conférences ou formations ont été allouées à d'autres priorités. Nous avons ainsi réalisé un atelier de travail avec un service ministériel et développé des activités de formation en e-learning. Nous avons aussi participé, le 28 janvier 2021, à la 15^{ème} Journée internationale de la protection des données, avec l'organisation d'une conférence préenregistrée sur le thème de la protection des données face à la numérisation du travail.

QUELLES VONT ÊTRE VOS PRIORITÉS DANS LES ANNÉES À VENIR ?

Nous avons plusieurs priorités pour 2022 et les années à venir : développer la communication externe et encore améliorer la visibilité de la CNPD auprès de toutes les cibles ; développer une communication plus visuelle et graphique, avec des outils adaptés ; poursuivre les actions entreprises précédemment vers le grand public et les acteurs du secteur privé et du secteur public ; développer des modules de formation pour les jeunes (avec une offre spécifique sur les protection des données dans le cadre du premier BTS spécialisé en cybersécurité mis en place au Luxembourg) ; développer un nouveau parcours de formation sur la protection des données à destination des agents du service public (en collaboration avec le CGPD et l'INAP) ; renouveler des modules d'initiation à la protection des données à destination des citoyens et enfin développer les ateliers DaProLab (Data Protection Laboratory) en présentiel pour les professionnels de la protection des données. ■

4

LES ACTIVITÉS EN 2021



Sensibilisation des jeunes étudiants en sécurité informatique

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 ont démarré à 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. Plusieurs collaborateurs de la CNPD participent en tant que formateurs aussi bien dans le cadre du cours d'introduction au RGPD que dans le cadre des ateliers de travail thématiques.

Nouveau parcours de formation INAP

Depuis 2021, la CNPD développe en coopération avec le Commissariat du gouvernement à la protection des données (CGPD) et l'Institut national

d'administration publique (INAP) un nouveau parcours de formation d'initiation à la protection des données personnelles basé sur les besoins des agents de la fonction publique. Il est prévu de mettre à disposition un module e-learning d'introduction au RGPD qui sera disponible sur la plateforme d'apprentissage de l'INAP au courant de l'année 2022 et qui a comme objectif de sensibiliser l'ensemble des agents sur les principes de base de la protection des données ainsi que le développement de modules de formation plus spécifiques sur certains thèmes choisis et dispensés en mode blended learning ou dans le format DaProLab. Ces modules ne seront mis en œuvre qu'à partir de 2023.

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

La diversification économique du pays par la recherche et l'innovation (RDI) est largement orientée vers le domaine des sciences numériques, de la cybersécurité, de l'intelligence artificielle et, en général, les technologies digitales innovantes.

La CNPD se doit donc 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 tant que membre du comité de suivi ou du comité de pilotage du projet :

- *DECEPTICON* : projet de recherche conjoint de l'Université de Luxembourg (SnT/IRiSC) avec et le LIST et cofinancé par le FNR ;
- *DAPROCADE (DAta PROtection CApability DEtermination)* : projet du LIST cofinancé par le FNR ;
- *PaCT (Privacy policy Certification and Translation)* : projet de transfert de technologie de l'Université de Luxembourg cofinancé par le FNR dans son programme JUMP PoC ;
- *National Digital Twin* : projet du LIST (Luxembourg Institute of Science and Technology) et cofinancé par le FNR ;
- *Smart Schoul 2025* : projet de sensibilisation de l'Université du Luxembourg (SnT) en collaboration avec le SCRIPT du Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse (MENJ), et le Lycée Edward Steichen Clervaux (LESC) cofinancé par le FNR.

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 pour le traçage des contacts par application mobile, la Contact Tracing App, qui n'a finalement pas vu le jour au Luxembourg.

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.

SPAMBEE : LA SOLUTION NATIONALE ANTI-SPAM ET ANTI-PHISHING

Développé conjointement par BEE SECURE, le Cybersecurity Competence Center Luxembourg (C3) et la CNPD, l'outil SPAMBEE permet aux utilisateurs de faire analyser de manière anonyme les e-mails suspects de spams ou de phishing (hameçonnage).

Le spam et les attaques de type « phishing » sont un stress permanent pour les utilisateurs et augmentent d'année en année. En effet, 130.0000 attaques de phishing ont été notifiées au Computer Incident Response Center Luxembourg (CIRCL) en 2020, dont on peut compter 4 % pour le Luxembourg.

SPAMBEE est un plug-in qui, une fois installé, permet à chacun, d'un simple clic, de fournir aux autorités et experts compétents des informations importantes pour lutter contre les cybercriminels. Le traitement des e-mails suspects alimente une base de données d'expéditeurs à bannir.

Cet outil protège les données personnelles conformément au RGPD, car seules les données techniques pertinentes pour l'analyse des e-mails sont transférées, pas le contenu, ni le nom du destinataire.

SPAMBEE est gratuit et peut être installé sur la plupart des navigateurs et des clients mail. Il est disponible en français, luxembourgeois, allemand et anglais.

4

LES ACTIVITÉS EN 2021

2 Répondre aux demandes d'information de particuliers et de professionnels

La Commission nationale a reçu 618 demandes d'information par écrit en 2021, soit une légère baisse par rapport à l'année précédente (-5 %). Lors des trois dernières années, le nombre des demandes est resté constant avec plus de 600 par an. L'entrée en application du RGPD avait provoqué le pic exceptionnel en 2018.

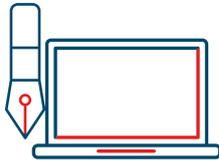
Environ la moitié des demandes d'information par écrit introduites en 2021 émanait de personnes physiques, confirmant une tendance déjà notée en 2020 alors qu'un tiers des requêtes provenaient d'entreprises privées. Les entités publiques, relevant du secteur étatique et communal, continuaient à solliciter régulièrement la Commission nationale sur un large éventail de questions.

Alors que les questions relatives aux traitements de données à caractère personnel concernant

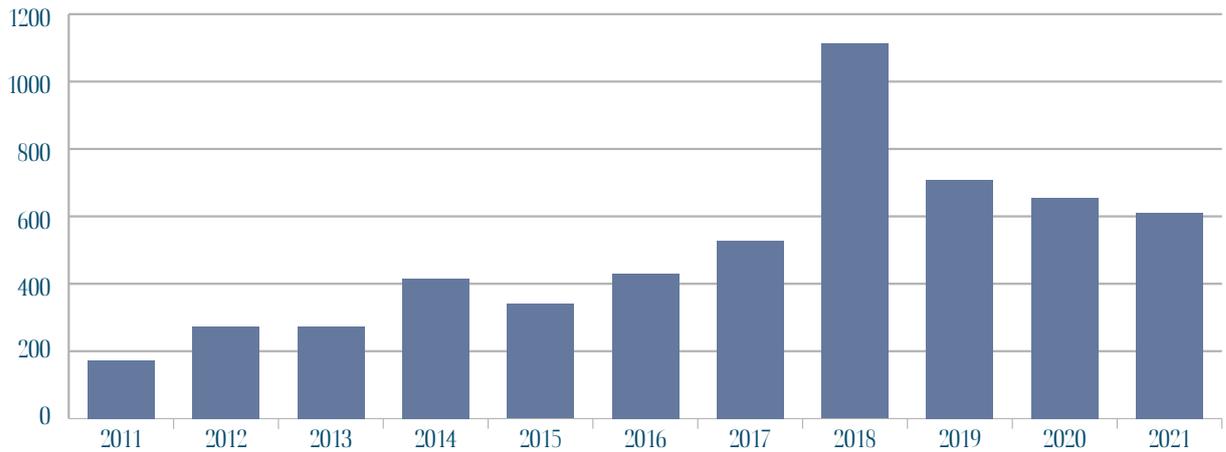
la gestion de la pandémie COVID-19 subsistaient, l'année 2021 a également été marquée par un retour à d'autres thématiques, notamment en lien avec la vidéosurveillance et la surveillance sur le lieu du travail. Les personnes concernées ont sollicité des informations sur l'exercice de leurs droits, en particulier du droit d'accès et du droit à l'effacement.

Les responsables du traitement se sont également interrogés sur les conditions de licéité du traitement, notamment les modalités du recueil du consentement, sur l'application des grands principes applicables en matière de mise en œuvre de traitements de données et sur des questions plus générales sur les obligations en matière de désignation d'un délégué à la protection des données et de la sécurité de l'information. Finalement, la Commission nationale a régulièrement été sollicitée au sujet des caractéristiques de traitements de données spécifiques à la gestion des ressources humaines, au secteur financier et dans le domaine de l'éducation.

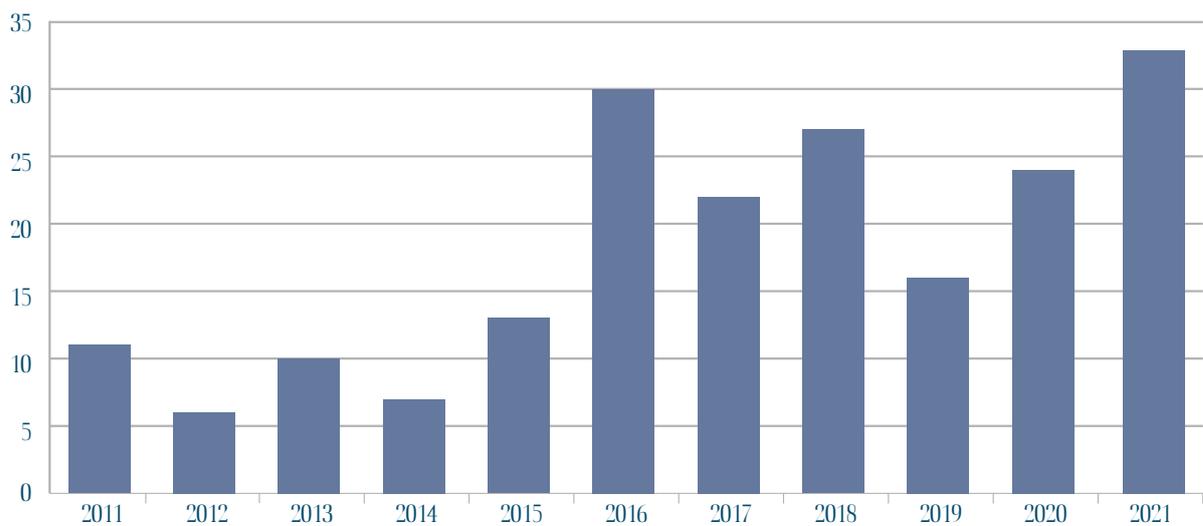
La CNPD informe et conseille les particuliers et les professionnels qui souhaitent obtenir des renseignements juridiques, des informations sur l'exercice de leurs droits ou une assistance à la mise en conformité de leurs traitements à la législation relative à la protection des données. Un service dédié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



ÉVOLUTION DU NOMBRE DE DEMANDES D'INFORMATION PAR ÉCRIT



ÉVOLUTION DU NOMBRE DES AVIS



4

LES ACTIVITÉS EN 2021

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 2021, la Commission nationale a émis 33 avis sur des projets de loi ou de règlements grand-ducaux, soit 9 de plus qu'en 2020.

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 notamment été abordées dans les avis de la CNPD :

- Lutte contre la pandémie COVID-19
- VISUPOL (Vidéosurveillance à des fins policières)
- Données ouvertes et réutilisation des informations du secteur public
- Contrôle de l'acquisition et de la détention d'armes
- Contrôle d'honorabilité
- Code des communications électroniques européen
- Fichier central de la Police grand-ducale
- Recensement général de la population, des logements et des bâtiments
- Organisation des services de taxis

- Régimes internes des centres pénitentiaires
- Connaissance de ses origines dans le cadre d'une adoption / procréation médicalement assistée avec tiers donneurs
- Carte de stationnement pour personnes handicapées

Par ailleurs deux avis en matière de surveillance sur le lieu du travail, ci-après désignés « avis travail », ont été adoptés en 2021 (procédure de l'article L.261-1 paragraphe (4) du Code du travail) sur l'enregistrement des sessions de travail à distance et le déploiement d'une application de collecte de données agrégées de productivité.

Finalement, 5 des 33 avis de la CNPD concernaient les traitements de données à caractère personnel en matière pénale, ainsi qu'en matière de sécurité nationale. Ces avis 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 2021, la CNPD voudrait mettre en avant les six 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>

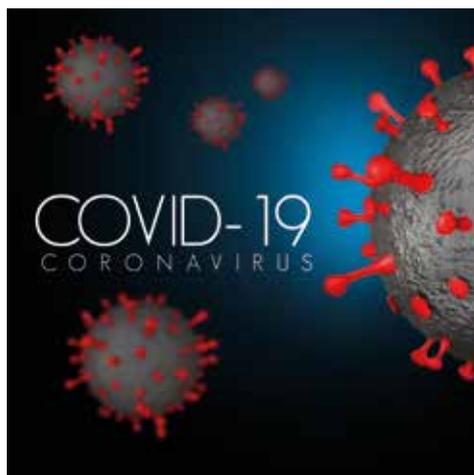
MESURES DE LUTTE CONTRE LA PANDÉMIE COVID-19

En 2021, la Commission nationale a adopté huit avis sur des projets ou propositions de loi ayant trait aux mesures de lutte contre la pandémie Covid-19.

La CNPD a notamment émis des observations concernant :

- les traitements des données personnelles dans le cadre du programme de dépistage à grande échelle et du programme de vaccination ;
- l'obligation pour les établissements du secteur Horeca de tenir un registre de leurs clients servant à faciliter le contact tracing. Les dispositions y afférentes du projet de loi n'ont cependant pas abouti ;
- l'instauration du régime Covid Check et plus particulièrement les informations rendues visibles lors de l'utilisation de l'application CovidCheck.lu, l'obligation de présenter une pièce d'identité et la possibilité d'établir une liste des personnes vaccinées et rétablies.

Dans ses avis, la Commission nationale a insisté sur le fait que les mesures législatives instaurant des traitements de données à caractère personnel devraient être claires et précises et que leur 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. Elle a également rappelé l'importance du principe de minimisation en vertu duquel les données personnelles collectées doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

DONNÉES OUVERTES ET LA RÉUTILISATION DES INFORMATIONS DU SECTEUR PUBLIC

La CNPD a rendu deux avis sur le projet de loi n°7643 sur les données ouvertes et la réutilisation des informations du secteur public qui a pour objet de transposer en droit national la directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public

4

LES ACTIVITÉS EN 2021

(refonte) ainsi que d'abroger et de remplacer la loi modifiée du 4 décembre 2007 sur la réutilisation des informations du secteur public.

En soulignant son attachement à l'intérêt public que représente l'accès du public aux documents officiels, la Commission nationale a formulé des observations visant à parvenir à la définition d'un cadre juridique où la réutilisation des données publiques et la protection de la vie privée et des données à caractère personnel trouvent un équilibre quand un document contenant des données à caractère personnel est susceptible d'être communiqué.

La CNPD s'est interrogée sur l'articulation du projet de loi avec les règles d'accès aux documents contenant des données à caractère personnel et a pointé vers le risque de divulgation de données à caractère personnel ou de l'atteinte à la vie privée des personnes physiques lorsque la législation sectorielle prévoyant l'accès aux documents est muette au sujet de la réutilisation de données à caractère personnel.

La Commission nationale a rappelé que les entités souhaitant réutiliser des informations du secteur public comprenant des données personnelles restent soumises aux dispositions en matière de protection des données à caractère personnel et doivent ainsi s'assurer que leur traitement de données est conforme au RGPD et aux autres dispositions législatives et réglementaires.

Enfin, dans l'optique d'un accès accru aux informations du secteur public et d'une future stratégie nationale pour la promotion de l'Open data au Luxembourg, la CNPD a souligné l'importance du concept de l'« ouverture dès la conception et par défaut » signifiant que les détenteurs de données publiques devraient concevoir lesdites données dans l'optique de rendre celles-ci réutilisables et notamment concevoir les jeux de données permettant la dissociation des données à caractère personnel au moment de la mise à disposition au public par le biais notamment de l'anonymisation et de l'application du principe de minimisation.

CODE DES COMMUNICATIONS ÉLECTRONIQUES EUROPÉEN

La Commission nationale a rendu un avis relatif au projet de loi n°7632 qui a pour objet de transposer la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

La CNPD a estimé nécessaire de modifier la définition des services de communications électroniques dans la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques afin d'y intégrer les opérateurs OTP « over the top players » offrant des services de communications interpersonnelles non fondés sur la numérotation.

Cette modification de la définition est requise afin d'assurer une transposition conforme de la directive (UE) 2018/1972. Elle est par ailleurs nécessaire afin de garantir le respect des droits fondamentaux, comme la directive et le projet de loi le prévoient.

La CNPD a également suggéré de préciser en détail les cas de figure dans lesquels jouent les obligations à charge des entreprises (qui fournissent un réseau ou un service de communications électroniques) en matière de facilitation de l'interception légale des communications par les autorités compétentes et de mise à disposition des données techniques aux autorités.

Par ailleurs, la CNPD a proposé de coordonner les procédures de l'ILR (Institut Luxembourgeois de Régulation) d'un côté et de la CNPD de l'autre pouvant aboutir à des sanctions administratives ainsi que de donner des détails sur la coopération entre les deux institutions qui est prévue par le projet de loi.

Enfin, la CNPD a suggéré de mettre en adéquation le projet et loi avec la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques en ce qui concerne les questions de la localisation des appels d'urgence, des factures détaillées et de l'identification de la ligne appelante.

PROCÉDURES DE CONTRÔLE D'HONORABILITÉ

La CNPD a rendu un avis sur le projet de loi n°7691 relatif aux procédures de contrôle d'honorabilité. Ce projet de loi a pour objet de préciser les différentes procédures de « contrôle d'honorabilité » prévues dans plusieurs textes de loi relevant de la compétence du ministre de la Justice.

Tout d'abord, la Commission nationale a regretté que le projet de loi ne propose pas de définition commune de la notion d'honorabilité ni n'instaure, pour les trois catégories d'enquêtes d'honorabilité visées par le projet de loi, un cadre légal uniformisé en ce qui concerne les acteurs qui diligentent de telles enquêtes et en ce qui concerne les modalités de transmission des informations issues de celles-ci.

La CNPD a ainsi estimé qu'il serait préférable que les enquêtes administratives soient diligentées par une même et seule autorité et qu'elles devraient être confiées à une autorité répressive, le Ministère public, et non pas à une/des administration(s). Ainsi, elle considère que les auteurs du projet de loi devraient opter pour un système qui se baserait sur la communication d'un avis circonstancié du procureur d'Etat général afin d'apprécier l'honorabilité des personnes concernées.

Par ailleurs, la CNPD a rappelé que les traitements de données à caractère personnel

4

LES ACTIVITÉS EN 2021

relatives aux condamnations pénales et aux infractions ou aux mesures de sûretés connexes devraient respecter les dispositions de l'article 10 du RGPD et que ceux relatifs à des catégories particulières de données se devraient de respecter l'article 9 du RGPD.

Enfin, elle a encore rappelé que les traitements de données visés par le projet de loi devraient respecter les grands principes visés à l'article 5, paragraphe (1) du RGPD. Pour une analyse concrète de chacun de ces principes par rapport aux dispositions légales du projet de loi, il est renvoyé à l'avis de la Commission nationale.

RECENSEMENT GÉNÉRAL DE LA POPULATION

La CNPD a rendu un avis sur le projet de règlement grand-ducal prescrivant un recensement général de la population, des logements et des bâtiments du Grand-Duché. Ce projet avait pour objet l'organisation du recensement général de la population, des logements et des bâtiments, qui a débuté le 8 novembre 2021.

Dans cet avis, la Commission nationale a fait part de ses interrogations quant à la conformité de la loi modifiée du 10 juillet 2011 portant organisation du STATEC par rapport aux règles applicables en matière de protection des données, et de ses observations quant à l'articulation entre les dispositions du chapitre 2 de la loi du 1^{er} août 2018 portant organisation de la Commission

nationale pour la protection des données et du régime général sur la protection des données, et celles de la loi modifiée du 10 juillet 2011 portant organisation du STATEC.

En ce qui concerne les acteurs impliqués dans le recensement, la Commission nationale a recommandé pour une meilleure lisibilité et compréhension du texte avisé, que soit précisé expressément dans le projet de règlement grand-ducal que le STATEC a la qualité de responsable du traitement, et de clarifier le rôle des communes dans le cadre du recensement.

Quant à la collecte de catégories particulières de données, la CNPD a rappelé que de tels traitements de données étaient soumis à des exigences plus strictes ainsi qu'à une protection spécifique en vertu de l'article 9 du RGPD. Elle a également relevé qu'il conviendrait de respecter, le cas échéant, les dispositions des articles 64 et 65 de la loi du 1^{er} août 2018 précitée en ce qu'elles prévoient des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Quant à la collecte du numéro d'identification national, la CNPD a estimé que son utilisation, telle que prévue par le projet de règlement grand-ducal devrait être encadrée par une loi, car un tel traitement n'était pas prévu par la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques. Par ailleurs, elle a

également souligné que des précisions quant au lien entre la « clé de recensement » et le numéro d'identification national de la personne recensée mériteraient d'être apportées alors que tant la « clé de recensement » que le numéro d'identification national ont pour objet de fusionner les données recueillies dans le cadre du recensement.

Quant à l'accès aux registres administratifs, la Commission nationale a noté que les modalités d'accès à ceux-ci devraient être plus précises.

Enfin, la CNPD a rappelé la nécessité de respecter les principes d'intégrité et de confidentialité, de limitation de conservation des données ainsi que les principes de licéité, de loyauté et de transparence vis-à-vis des personnes concernées.

ACCÈS À LA CONNAISSANCE DE SES ORIGINES

La Commission nationale a émis un avis relatif au projet de loi n°7674 portant organisation de l'accès à la connaissance de ses origines dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs. N'ayant pas été saisie directement par les auteurs du projet de loi, l'autosaisine de la CNPD est intervenue dans le cadre des nombreux traitements de données à caractère personnel, entre autres de données de santé, réalisés aux fins de l'exercice de l'accès à la connaissance

de ses origines et affectant les aspects les plus intimes de la vie privée des personnes concernées.

La Commission nationale a fait observer l'insécurité juridique liée à l'imprécision des termes employés dans le projet de loi et a estimé que le texte ne respecterait 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. De même, l'avis de la CNPD souligne la nécessité de définir clairement le rôle des différents intervenants.

Finalement, la Commission nationale a insisté sur l'importance d'assurer l'intégrité et la confidentialité des données dans la mesure où des accès non-autorisés aux données, des fuites de données ou encore des modifications non-désirées de données sont susceptibles de causer un préjudice grave aux personnes concernées.

4

LES ACTIVITÉS EN 2021

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 traitent. 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 spécifique.

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 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 CNPD¹ à plusieurs reprises en tenant compte de l'évolution des textes légaux en relation avec la pandémie.

Celles-ci ont été complétées en 2021 par une foire aux questions (FAQ) sur la protection des données dans le contexte du CovidCheck (tel que prévu par la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19). Elle y répond aux questions fréquemment posées concernant notamment l'utilisation de l'application CovidCheck.lu et décrit ce que peut faire l'employeur dans le cadre de la mise en place du CovidCheck sur le lieu du travail.

LIGNES DIRECTRICES EN MATIÈRE DE GÉOLOCALISATION DES VÉHICULES MIS À LA DISPOSITION DES SALARIÉS

Les systèmes de géolocalisation des véhicules mis à la disposition des salariés permettent aux employeurs de suivre les déplacements de leurs salariés dans le temps et dans l'espace. De tels systèmes sont aujourd'hui largement répandus aussi bien dans les entreprises que dans les organisations publiques souvent pour pouvoir gérer la flotte des véhicules utilitaires et l'optimisation de l'organisation

¹ <https://cnpd.public.lu/fr/actualites/national/2020/03/coronavirus.html>



du travail. Cependant, comme l'utilisation de ces dispositifs implique un traitement de données à caractère personnel, il comporte des risques pour la vie privée des salariés. Ainsi, la géolocalisation expose les salariés au risque d'être suivis en temps réel par leur employeur en dehors des périodes de travail, ou encore au risque que le système de géolocalisation soit utilisé par l'employeur pour des finalités autres que celles pour lesquelles il a été installé.

Sans vouloir prétendre à l'exhaustivité, la CNPD tient à rappeler dans ces lignes directrices certains des principes et obligations applicables en matière de géolocalisation des salariés au regard de la législation applicable en matière de protection des données à caractère personnel.

LIGNES DIRECTRICES EN MATIÈRE DE COOKIES ET AUTRES TRACEURS

Ces lignes directrices ont pour but d'aider les opérateurs de sites internet ou d'applications

à se conformer aux règles actuellement applicables, telles qu'elles ressortent de la législation et de la jurisprudence existantes.

L'exploitation d'un site internet nécessite souvent l'utilisation de témoins de connexion (appelés communément « cookies ») ou d'autres technologies similaires.

Ceux-ci peuvent être propres au site internet ou bien être déposés/lus par des tiers (plateformes vidéo, social plugins, régies publicitaires, besoins analytiques, etc.) sur le terminal de l'utilisateur dans le cadre de services utilisés par le site internet.

Ces cookies et technologies similaires peuvent être utilisés afin de poursuivre des finalités plus ou moins intrusives dans la vie privée des internautes, comme par exemple se souvenir du choix de langue d'un utilisateur ou bien suivre son comportement de navigation sur internet.

Dans ses lignes directrices, la CNPD analyse le contexte juridique et formule des observations sur les cookies essentiels (pour lesquels il n'y a pas d'obligation de consentement) et sur les cookies non essentiels (pour lesquels il y a une obligation de consentement). Elles introduisent également la notion de « dark patterns » dans le contexte du recueil du consentement des utilisateurs. En outre, les lignes directrices contiennent de nombreux exemples de bonnes pratiques.

4

LES ACTIVITÉS EN 2021

5 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.

En 2021, 120 responsables du traitement ont communiqué les coordonnées de leur DPD à la Commission nationale. Depuis le 25 mai 2018, 1329 responsables du traitement ont effectué cette démarche.

Au total, 1011 personnes physiques ou morales ont été déclarées auprès de la CNPD, dont 164 en 2021.

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

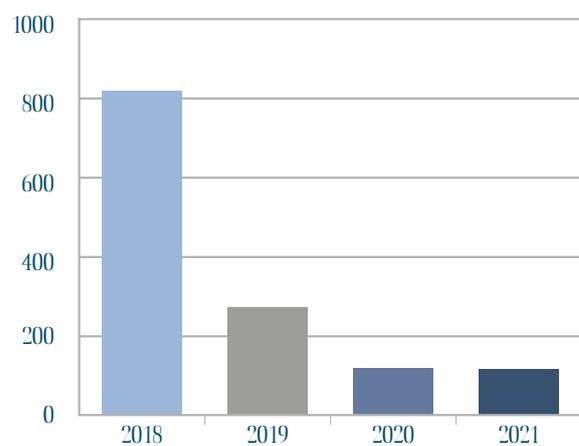
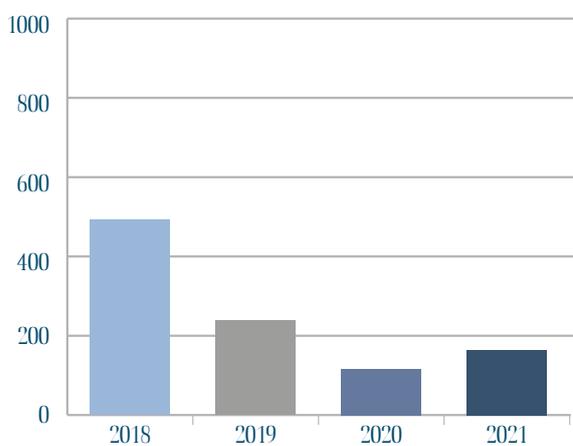


leur nature, de leur portée et/ou de leurs finalités, exigent un **suivi régulier et systématique à grande échelle** des personnes concernées ;

- 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.

**PERSONNES PHYSIQUES OU MORALES
DÉCLARÉES AUPRÈS DE LA CNPD
EN TANT QUE DPO**



**RESPONSABLES DE TRAITEMENTS QUI
ONT COMMUNIQUÉS LES COORDONNÉES
DE LEUR DPO À LA CNPD**

4

LES ACTIVITÉS EN 2021



ALAIN HERRMANN
Commissaire

«
...nous faisons
figure de pionniers.»
»

MONSIEUR HERRMANN, VOUS AVEZ LA CERTIFICATION RGPD PARMİ VOS DIVERSES ATTRIBUTIONS. POUVEZ-VOUS NOUS EXPLIQUER DE QUOI IL S'AGIT ?

Alain Herrmann : Le RGPD – Règlement Général sur la Protection des Données – est entré en vigueur dans l'Union européenne en 2018. Ce règlement donne entre autres la possibilité d'adopter des schémas de certification. Le Luxembourg a fait office de pionnier européen : nous sommes actuellement le seul pays de l'Union européenne à disposer d'une telle certification. Il s'agit d'un outil, basé sur des critères exigeants, permettant de répondre aux besoins des professionnels qui veulent démontrer à leurs partenaires commerciaux, à leurs clients... qu'ils respectent le RGPD dans toutes leurs opérations de traitement des données.

QUEL EST L'INTÉRÊT POUR UNE ENTREPRISE DE DISPOSER D'UNE TELLE CERTIFICATION ?

L'intérêt est multiple, sachant toutefois que ce n'est pas une entreprise en tant que telle qui est certifiée, mais le traitement des données qu'elle effectue. Cela étant précisé, si une entreprise dispose d'une telle certification, cela démontre qu'elle accorde de l'importance au traitement des données qu'elle possède et qu'elle se conforme au RGPD. Des mécanismes de certification RGPD peuvent aussi être utiles dans les relations commerciales entre entreprises, par exemple entre le responsable du traitement et son sous-traitant. Enfin, le fait de posséder cette certification renforce une image de marque et peut même constituer une sorte d'avantage concurrentiel. La certification permet à l'entreprise qu'il l'a obtenue de se distinguer au sein de son secteur d'activité.

ET QUELS SONT LES AVANTAGES POUR LES CITOYENS ?

On peut résumer cela en un mot : confiance. Lorsqu'un citoyen est en relation avec une entreprise bénéficiant de cette certification, ce citoyen sait que ses données sont traitées dans le respect du RGPD. Pour le citoyen, c'est une véritable garantie sachant que le

système de certification mis en place a été conçu pour minimiser le risque d'utilisation abusive de ses données à caractère personnel. C'est rassurant.

LE CNPD EST LA PREMIÈRE AUTORITÉ AU SEIN DE L'UNION EUROPÉENNE À AVOIR ÉLABORÉ SES PROPRES CRITÈRES DE CERTIFICATION. POUVEZ-VOUS NOUS EXPLIQUER BRIÈVEMENT LE PROCESSUS QUI A PERMIS AU CNPD ET AU LUXEMBOURG DE DEVENIR PIONNIERS EN LA MATIÈRE ?

Effectivement, nous faisons figure de pionniers. Mais aussi de cobayes, si je puis dire. Lorsque le RGPD est entré en vigueur, laissant la possibilité d'adopter des schémas de certification, nous avons tout de suite compris l'intérêt à mettre en place une telle certification. Le processus a été long et difficile parce que nous partions d'une page blanche. Il nous fallait donc développer la certification, déterminer les critères d'attribution... dans le respect du RGPD tout en privilégiant un haut niveau d'exigence. Nous devions aussi agir en parfaite intelligence avec les autres autorités européennes pour développer un système intégré sérieux, fiable et qualitatif. Finalement, nous avons reçu un avis européen favorable. C'était le 2 février 2022.

LE CNPD ÉTANT UN PIONNIER, VOTRE EXPÉRIENCE DOIT ÊTRE UTILE AU NIVEAU EUROPÉEN. COMMENT CONTRIBUEZ-VOUS AUX TRAVAUX EUROPÉENS EN LA MATIÈRE ?

Le CNPD a établi des critères strictes permettant à notre certification d'avoir un haut niveau de protection des données et de qualité. En tant que premier pays européen à avoir adopté une certification nationale, nous avons développé des connaissances, une expérience et un savoir-faire que nous mettons volontiers à la disposition de nos partenaires européens. Si nécessaire, nous sommes prêts à étudier la possibilité d'étendre le schéma innovant que nous avons développé au niveau comité européen et, d'ailleurs, nous sommes actifs au niveau du board européen de la protection des données. ■

4

LES ACTIVITÉS EN 2021

6 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 telles que proposées dans le RGPD. Ces instruments peuvent servir aux responsables du traitement et sous-traitants d'éléments pour démontrer que leurs opérations de traitement respectent le règlement.



La mise en place de mécanismes de certification volontaires peut favoriser la transparence et le respect du RGPD et permettre aux personnes concernées de mieux 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 la certification 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 (EDPB) à :

- l'adoption des critères de certification et
- l'adoption d'un label européen pour la certification.

La CNPD est la première autorité de protection des données en Europe à soumettre ses critères de certification à l'EDPB pour avis en octobre 2021 et, une fois ces critères adoptés, le Luxembourg sera le premier pays à permettre la certification selon les critères du RGPD.

Procédure d'agrément des organismes de certification

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.

La CNPD a déjà reçu 2 candidatures d'entreprises qui souhaitent recevoir cet agrément comme organisme de certification au Luxembourg (sous le régime des critères d'agrément CARPA de la CNPD). La CNPD est en train d'analyser ces candidatures en phase préliminaire et va pouvoir commencer des audits d'agrément en 2022.

Rapporteur au niveau européen

Au cours des dernières années, la CNPD était rapporteur sur les guidances concernant les critères de certification au niveau de l'EDPB.

En 2021, il s'agissait d'un addendum aux lignes directrices 1/2018 sur la certification et l'identification des critères de certification conformément aux articles 42 et 43 du RGPD.

L'objectif de cette guidance supplémentaire était d'affiner les éléments des lignes directrices 1/2018 afin d'aider :

- les parties prenantes impliquées dans la rédaction des critères de certification dans le cadre de la certification RGPD et ;

4

LES ACTIVITÉS EN 2021

- les autorités de contrôle et l'EDPB afin d'être en mesure de fournir des évaluations cohérentes dans le contexte de l'approbation des critères de certification (tant pour les systèmes nationaux que pour les labels de protection des données de l'UE).

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 instrument de gouvernance utile et efficace en fournissant une description détaillée de l'ensemble des comportements les plus appropriés et reprenant les meilleures pratiques dans un secteur donné.

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

En 2021, la CNPD a reçu une initiative de code de conduite qu'elle est en train d'analyser.

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

Une AIPD ou DPIA en 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 doit contribuer 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* ») étant donné qu'elle aide les responsables de traitement à identifier et à traiter les problèmes à un stade précoce et qu'elle contribue à démontrer leur conformité.

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 cas².

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 2021, seulement une demande d'avis préalable a été soumise à la CNPD. Ce chiffre très peu

² La liste peut être consultée sur le site Internet de la CNPD : <https://cnpd.public.lu/fr/professionnels/obligations/AIPD.html>

élevé en comparaison avec ceux des pays limitrophes indique que l'utilisation des AIPD ne semble pas encore être très répandue parmi les responsables du traitement établis au Luxembourg.



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).

Publication de nouvelles clauses contractuelles types de la Commission européenne

La Commission européenne a publié le 4 juin 2021 de nouvelles clauses contractuelles types (CCT) destinées à encadrer les transferts de données des responsables de traitement ou des sous-traitants de l'UE/EEE (soumis au RGPD) à des responsables du traitement ou des sous-traitants établis en dehors de l'UE/EEE (et non soumis au RGPD).

Les nouvelles CCT remplaceront les anciennes qui étaient adoptées sur la base de la directive 95/46 sur la protection des données.

Les versions précédentes des CCT ont dû être mises à jour afin de les mettre en conformité avec les exigences du RGPD, ainsi que pour tenir compte de l'arrêt « Schrems II » de la CJUE, et mieux refléter le recours généralisé à de nouvelles opérations de traitement plus complexes impliquant souvent de multiples importateurs et exportateurs de données.

En particulier, les nouvelles CCT prévoient des garanties plus spécifiques dans le cas où les lois du pays de destination ont une incidence sur le respect des clauses, notamment en cas de demandes contraignantes de la part des pouvoirs publics en vue de la divulgation de données à caractère personnel.

4

LES ACTIVITÉS EN 2021

Elles peuvent être utilisées par les entreprises, organismes publics et associations luxembourgeoises qui entendent transférer certaines données qu'ils sont amenés à traiter vers des pays tiers (en dehors de l'UE/EEE).

Une période de transition est toutefois prévue pour pouvoir continuer à invoquer les anciennes clauses contractuelles types adoptées sur base de la directive 95/46 sur la protection des données, jusque fin 2022.

Adoption par la Commission européenne de deux décisions relatives à l'adéquation du niveau de protection des données concernant le Royaume-Uni

Le 28 juin 2021, la Commission européenne a constaté par le biais de deux décisions d'adéquation que le Royaume-Uni assure un niveau de protection adéquat en matière de protection des données à caractère personnel, conformément au règlement général sur la protection des données et à la directive relative à la protection des données en matière pénale ainsi qu'en matière de sécurité nationale.

Une telle décision signifie que le régime de protection des données personnelles au Royaume-Uni offre des garanties « essentiellement équivalentes » à celles de l'Union européenne et que les transferts de données à caractère personnel vers le Royaume-Uni pourront de nouveau être effectués comme s'il s'agissait d'un transfert au sein de l'Espace économique européen.

Adoption d'une décision d'adéquation avec la Corée du Sud

Le 17 décembre 2021, la Commission européenne a constaté par le biais d'une décision d'adéquation que la République de Corée assure un niveau de protection adéquat en matière de protection des données à caractère personnel, conformément au règlement général sur la protection des données.

A noter que cette décision d'adéquation ne s'applique toutefois pas pour les transferts de données à caractère personnel en matière de crédit vers des entités sud-coréennes soumises à la surveillance de la Commission des services financiers, ni pour les transferts de données vers des organisations religieuses ou des partis politiques.

Dans ces cas, le régime général applicable aux transferts de données vers des pays tiers ne bénéficiant pas d'un niveau adéquat en matière de protection des données continuera à s'appliquer.

La CNPD contribue aux activités du Comité européen de la protection des données (EDPB).

A cet égard, l'autorité luxembourgeoise a été impliquée dans l'évaluation de cette décision d'adéquation de la Commission européenne en examinant le travail réalisé par cette dernière et en appréciant l'impact de la libre circulation des données à caractère personnel entre l'Union

européenne et la Corée du Sud sur les garanties et le degré de protection conférés par les deux économies aux citoyens européens.

Le 24 septembre 2021, l'EDPB a adopté son opinion sur la décision d'adéquation, qui est la troisième à avoir été adoptée sous l'égide du RGPD après celle du Japon et du Royaume-Uni.

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 2021, la CNPD a traité des dossiers concernant les règles d'entreprise contraignantes (BCRs, article 47 du RGPD) dont 8 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), 2 en qualité d'autorité secondaire (« *co-reviewer* ») (c'est-à-dire en appui de l'autorité de contrôle principale) et plusieurs en qualité d'autorité concernée.

4

LES ACTIVITÉS EN 2021



THIERRY LALLEMAND
Commissaire

...nous traitons
chaque réclamation
qui nous parvient.

LA CNPD REÇOIT PLUSIEURS CENTAINES DE RÉCLAMATIONS CHAQUE ANNÉE. QUELS SONT LES MOTIFS INVOQUÉS ?

Thierry Lallemand : Les réclamations sont déposées par des citoyens, des internautes ou des associations représentant des citoyens qui estiment que leurs droits en matière de protection des données n'ont pas été respectés ou qu'il y a un non-respect des réglementations en vigueur. Un autre motif concerne le droit d'accès des citoyens aux données les concernant. Le droit d'effacement (« droit d'oubli ») et le droit de rectification sont aussi des motifs récurrents. Les réclamations peuvent aussi concerner de mauvaises pratiques qui sont le fait d'entreprises du secteur privé ou d'organismes ou administrations du secteur public.

INTRODUIT EN 2018, LE RGPD A-T-IL EU UNE INFLUENCE SUR LE NOMBRE DE RÉCLAMATIONS ?

Nous constatons une augmentation du nombre de réclamations depuis l'introduction du RGPD. En 2017, nous avons enregistré 200 plaintes ; en 2018, année d'introduction du RGPD, nous avons totalisé 450 plaintes ; depuis 2 ou 3 ans, nous sommes à une moyenne annuelle d'environ 520 réclamations. L'introduction du RGPD a eu un impact sur le nombre de réclamations. Mais, du fait des campagnes de sensibilisation menées notamment par la CNPD, les citoyens sont mieux informés. C'est une bonne chose, mais cela entraîne aussi une hausse du nombre de réclamations.

QUELLE EST LA PROCÉDURE LORSQUE LA CNPD REÇOIT UNE RÉCLAMATION ?

J'insiste sur le fait que nous traitons chaque réclamation qui nous parvient. D'abord, nous analysons les faits. Nous voyons si la réclamation est fondée et recevable ou non. Nous étudions aussi l'importance de la violation de la législation et déterminons si la réclamation concerne une seule personne ou si elle peut avoir des répercussions sur un grand nombre de citoyens. Dans une première étape, nous tentons toujours de résoudre le problème à l'amiable.

QUAND UNE SOLUTION À L'AMIABLE N'EST PAS POSSIBLE, LA CNPD OUVRE UNE ENQUÊTE. QUEL EST LE PROCESSUS ?

L'ouverture d'une enquête est une procédure lourde qui demande des ressources et du temps. C'est l'un des commissaires de la CNPD qui propose l'ouverture d'une enquête quand il faut envisager des mesures contraignantes et coercitives. Il faut encore faire une distinction entre les enquêtes spécifiquement luxembourgeoises et celles à caractère européen. Le Luxembourg étant le siège européen d'entreprises d'envergure internationale, environ 30 % des réclamations que nous recevons sont le fait de non-résidents luxembourgeois. Dans ce cas, la procédure est encore plus compliquée car, même si la CNPD joue le rôle de chef de file, nous devons aboutir à un consensus avec toutes les autorités concernées. Si nous n'obtenons pas de consensus, c'est à l'EDPB (European Data Protection Board) d'arbitrer et de fournir une décision que nous appliquons.

SI UNE RÉOLUTION À L'AMIABLE N'EST PAS TROUVÉE, QUELLES SONT LES « ARMES » DE LA CNPD ?

Cela va du rappel à l'ordre à l'amende administrative, en passant par un avertissement, une suspension ou une interdiction temporaire du traitement des données. Il est aussi possible d'envisager l'interdiction définitive du traitement des données. Grâce au RGPD, notre nouvelle « arme » est l'amende administrative qui ne peut être appliquée qu'aux entreprises du secteur privé. Les administrations (État, ministères, communes...) sont exemptes d'amende administrative.

PUBLIEZ-VOUS LES RÉSULTATS DE VOS ENQUÊTES OU DES SANCTIONS APPLIQUÉES ?

Ces résultats sont publiés sur notre site Internet de manière anonyme : nous ne citons pas les entreprises, administrations... sur lesquelles nous avons enquêté ou auxquelles nous avons infligé une amende. Il est toutefois prévu que nous puissions effectuer des publications nominatives. Mais cela ne peut se faire qu'après épuisement de tous les recours et sans porter préjudice à l'entreprise nommée. ■

4

LES ACTIVITÉS EN 2021



Lorsqu'un responsable du traitement ne répond pas à l'exercice d'un droit tel que conféré par le RGPD ou lorsque la personne concernée estime qu'un traitement de données est effectué de manière illicite, elle peut introduire une réclamation auprès de la CNPD. En effet, la CNPD a, dans le cadre de ses missions, le devoir d'instruire les réclamations émanant des personnes concernées.

7 Traiter les réclamations des citoyens

Dans un premier temps, la CNPD examine si la réclamation est recevable par exemple en vérifiant 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.

Dans le cas où la réclamation est recevable, la CNPD prend contact avec le responsable du traitement et lui demande de prendre position et, le cas échéant, de se mettre en conformité et/ou de respecter les droits des personnes concernées.

Dans le cadre de la gestion des « réclamations » et lorsqu'un traitement de données litigieux est effectivement contraire à la législation, la CNPD s'efforce, dans une première étape, d'y remédier 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.

De plus, 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 2021, la CNPD a reçu un total de 512 réclamations :

- 360 réclamations ont été introduites directement auprès de la CNPD ;
- 152 réclamations ont été traitées via le système européen de coopération (IMI). En effet, la CNPD est compétente pour recevoir des réclamations émanant des autres autorités de contrôle européennes lorsque les responsables du traitement ont leur siège social au Luxembourg (autorité chef de file).

4

LES ACTIVITÉS EN 2021

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.

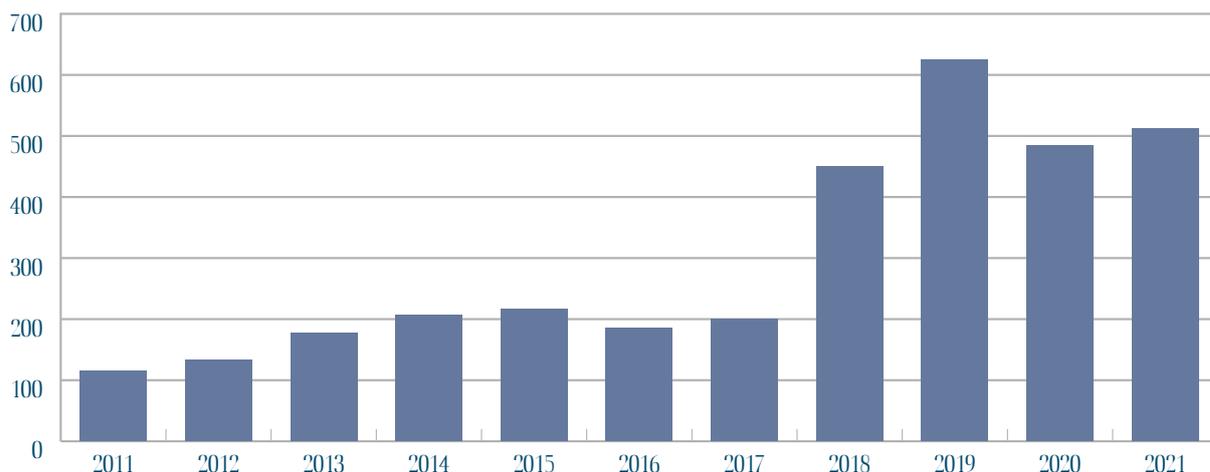
A l'aide du système IMI, les autorités de contrôle peuvent notamment :

- 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.

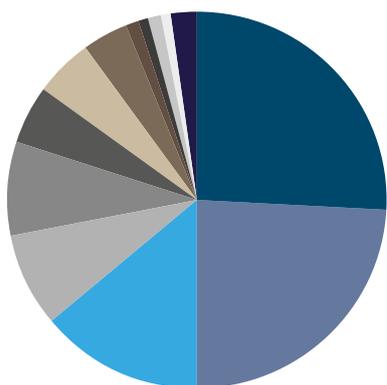


ÉVOLUTION DU NOMBRE DE RÉCLAMATIONS

Par rapport à l'année précédente, il s'agit d'une augmentation de 27 réclamations. Depuis l'entrée en application du RGPD en 2018, la CNPD traite en moyenne 518 réclamations par année.



MOTIFS DES RÉCLAMATIONS



- Refus d'accéder aux données (26 %)
- Demande d'effacement ou de rectification non respectée (24 %)
- Licéité du traitement (14 %)
- Opposition à prospection ou plaintes contre le spam (8 %)
- Violation des données (8 %)
- Vidéosurveillance (5 %)
- Consultation RNPP (5 %)
- Droit à l'information (4 %)
- Mesure de sécurité (1 %)
- Droit à l'image (1 %)
- Cookies (1 %)
- Durée de conversation (1 %)
- Autres (2 %)

4

LES ACTIVITÉS EN 2021

Plus d'un quart des réclamations (26 %) concerne 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 informations à communiquer lors de l'exercice d'un droit d'accès.

Les **demandes d'effacement ou de rectification** de données constituent 24 % des réclamations reçues. Il s'agissait, entre autres, de demandes de fermeture de comptes auprès de services/commerces en ligne ou de demandes d'effacement de données personnelles (adresses e-mail, évaluations, etc.) accessibles sur des sites Internet (comme des annuaires par exemple).

Dans 14 % 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.

8 % des réclamations concernent le **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.

La **transmission non autorisée de données à des tiers** a également conduit à un certain nombre de réclamations (8%). 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 »).

5 % des réclamations concernaient des demandes de vérification de licéité de consultations effectuées par des agents du secteur public au registre national des personnes physiques (RNPP).

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

DEMANDES DE MISE EN CONFORMITÉ

En 2021, 53 réclamations nationales ont conduit à des recommandations 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 (p. ex. faire droit à une demande d'accès, d'effacement, d'opposition, modification des notices, mise en place de mesures de sécurité supplémentaires, etc.) sans avoir dû déclencher une procédure d'enquête formelle.

Aux réclamations clôturées au niveau national, s'ajoutent à travers le système européen de coopération encore 86 réclamations qui ont été clôturées par des demandes de mise en conformité.

4

LES ACTIVITÉS EN 2021

8 Analyser les violations de données

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.

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

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 total d'incidents de sécurité en rapport avec des données à caractère personnel qui se produisent dans les organisations et 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 2021, 333 violations de données ont été notifiées à la CNPD, soit 46 de moins qu'en 2020.

Au total, depuis l'entrée en application du RGPD le 25 mai 2018, la Commission nationale a reçu 1238 violations de données. Cela correspond à une moyenne de 29 notifications de violations de données par mois.

Comme en 2020, la CNPD a constaté :

- que le secteur de la santé a rencontré un nombre significatif d'incidents de sécurité, un état encore accentué par la pandémie du COVID-19 et les traitements informatiques y relatifs. Toutefois, la CNPD note les efforts de ce secteur afin de traiter et de prévenir ces incidents.
- qu'elle ne reçoit pas ou peu de notifications des organismes issus du domaine des banques et assurances, pourtant de taille significative.
- que 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.

La principale cause de violation de données à caractère personnel reste **l'erreur humaine** (acte interne non malveillant) dans 62 % 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 plus d'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.

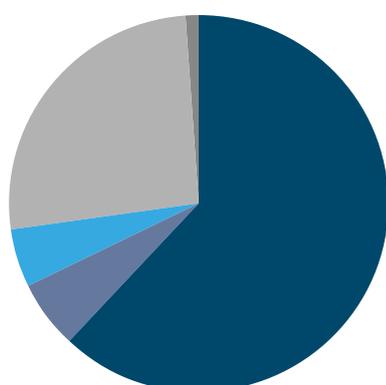
Les autres cas de figure sont liés à des bugs techniques qui résultent souvent dans la divulgation de données à caractère personnel à des tiers non autorisés (ex : mise en place ou mise à jour d'un nouveau service en ligne, cas non prévu d'utilisation d'un service, ...).

4

LES ACTIVITÉS EN 2021

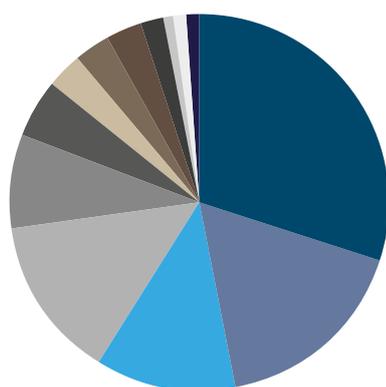


CAUSES DES VIOLATIONS



- Acte interne non malveillant (62 %)
- Acte interne malveillant (6 %)
- Acte externe non malveillant (5 %)
- Acte externe malveillant (26 %)
- Autre (1 %)

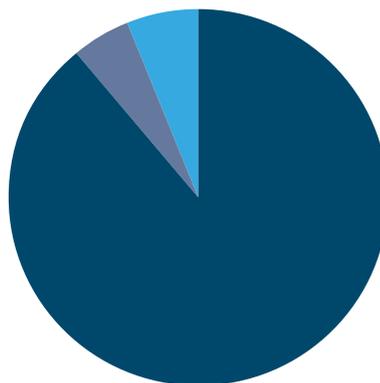
NATURE DES INCIDENTS



- Données à caractère personnel envoyé au mauvais destinataire (30 %)
- Piratage, hacking (17 %)
- Publication involontaire (12 %)
- Divulgence de la donnée personnelle de la mauvaise personne (14 %)
- Dispositif perdu ou volé (8 %)
- Phishing, hameçonnage (5 %)
- Problème technique (3 %)
- Papiers perdus, volés, endroit non sécurisé (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

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

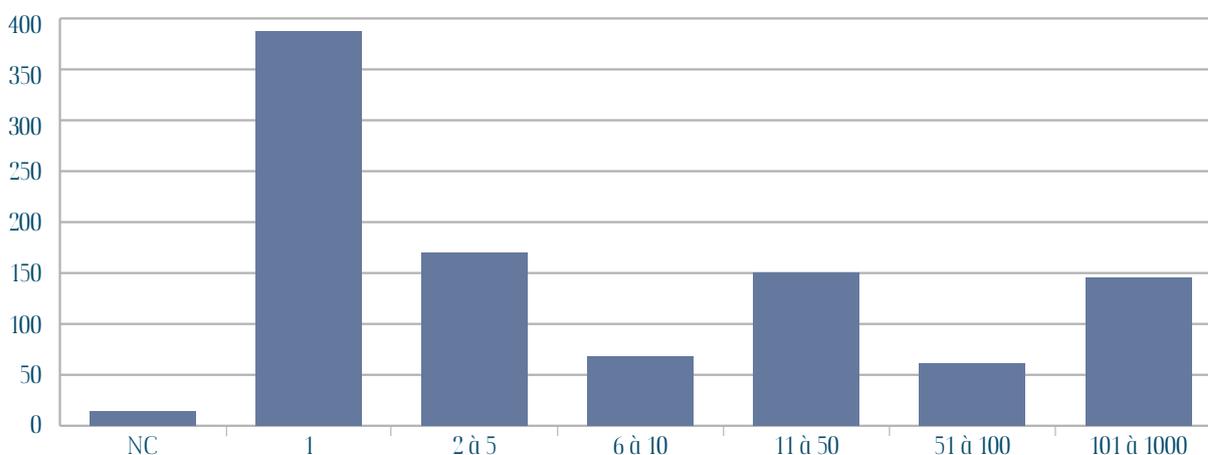


- Confidentialité (89 %)
- Disponibilité (5 %)
- Intégrité (6 %)

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)

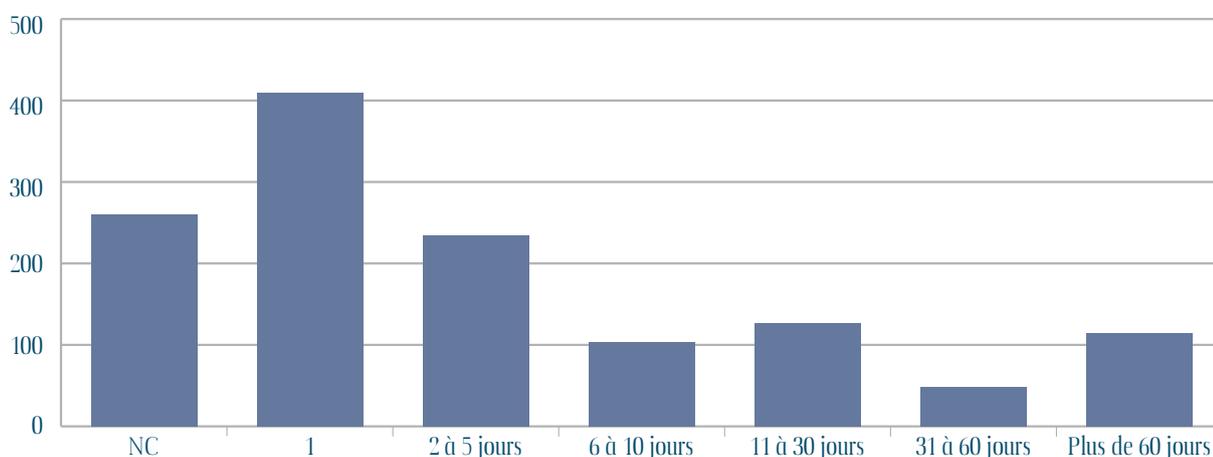


4

LES ACTIVITÉS EN 2021

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

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



Plus de la moitié des incidents de sécurité sont détectés 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.

La Commission nationale dispose de pouvoirs d'enquête afin de veiller au respect de la législation applicable en matière de protection des données. En cas de traitement contraire à la réglementation, la CNPD peut adopter des mesures correctrices y inclus des amendes financières.

9 Contrôler et adopter des mesures correctrices

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 forme de visites 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 notamment prendre la forme de campagnes de visites 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.

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 visites sur place proactives dans le cadre de campagnes thématiques (vidéosurveillance, géolocalisation et COVID-19 – voir ci-après) ou des visites sur place réactives 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 18 visites sur place en 2021, contre 8 en 2020.

La grande majorité de ces contrôles concernaient la 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

4

LES ACTIVITÉS EN 2021



dolor, sit amet consectetur adipiscing
hismod tempor incididunt ut labore et
aliqua. Ut enim ad minim veniam, quis
exitation ullamco laboris nisi ut aliquip
edo consequat. Duis aute irure dolor in
t in voluptate velit esse cillum dolore eu
ariatur. Excepteur sint occaecat cupidata
c sunt in culpa qui officia deserunt mollit
borum.

spécifiques en termes de protection des données induits par la pandémie. Les visites sur place 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 la méthodologie d'audit, particulièrement bien adaptée aux enquêtes 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 visites sur place, les enquêtes sous forme d'audits peuvent être organisées 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 thématiques 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.

Ensuite, la CNPD a poursuivi les enquêtes thématiques relatives à la **transparence** qui ont été lancées en 2020 auprès de 6 entreprises du secteur du commerce électronique. La transparence est un principe bien ancré 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 principe de la responsabilisation (« accountability »), auquel elle est intrinsèquement liée. La transparence doit permettre aux personnes concernées d'avoir un contrôle sur l'utilisation par le RT de leurs données à caractère personnel et d'exiger des responsables de traitement qu'ils rendent des comptes à cet égard. L'année 2021 a permis de finaliser les rapports d'enquête et de préparer les communications des griefs.

L'année 2021 marque également la fin du premier audit thématique sur la fonction de **délégué à la protection des données** (DPD). La Formation Restreinte de la CNPD a pris toutes les 25 décisions de cette campagne dont l'objectif était de vérifier la conformité des organismes aux obligations du RGPD en matière de désignation du DPD, de ses missions et de ses fonctions. Un rapport public avec les conclusions de cette campagne thématique va être publié en 2022.

4

LES ACTIVITÉS EN 2021

DÉCISIONS SUR L'ISSUE D'ENQUÊTES

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 20 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 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Avant que ladite formation restreinte prend une telle décision, une audience lui permet d'entendre aussi bien le chef d'enquête que le contrôlé qui pourront présenter des observations orales sur l'affaire et répondre à d'éventuelles questions de la part de la formation restreinte.

Les **premières décisions** de la Commission nationale siégeant en formation restreinte sur l'issue d'enquêtes menées depuis 2018 ont été prises en 2021. 49 dossiers ont pu être clôturés par la Commission nationale siégeant en formation restreinte, avec ou sans mesures correctrices ou amendes (12 clôturées en l'absence de manquements retenus, 37 avec mesures correctrices dont 25 avec amendes). Parmi ces dossiers, 48 décisions concernaient une affaire purement nationale (total de 319.500 € d'amendes administratives) et une décision était issue de la coopération européenne conformément aux articles 60 et suivants du RGPD (avec une amende administrative de 746.000.000 €).

Des 49 dossiers, 20 décisions concernaient le traitement de données opéré à travers un système de **vidéosurveillance et / ou par un dispositif de géolocalisation**.

Dans la majorité des décisions, la Commission nationale siégeant en formation restreinte a

constaté que les personnes concernées n'étaient pas suffisamment informées sur le traitement de leurs données à caractère personnel conformément aux dispositions de l'article 13 du RGPD.

Dans d'autres desdites décisions, une non-conformité à l'article 5.1.c) du RGPD (principe de minimisation des données) a été retenue, car les champs de vision des caméras installées par le contrôlé permettaient une surveillance continue et permanente sur le lieu de travail des salariés. La Commission nationale siégeant en formation restreinte ne nie pas que dans certains cas, il peut paraître nécessaire pour un responsable du traitement d'installer un système de vidéosurveillance sur le lieu de travail. Par contre, elle souligne toujours dans ses décisions qu'afin de respecter le principe de proportionnalité, le responsable du traitement doit recourir aux moyens de surveillance les plus protecteurs de la sphère privée du salarié en limitant, par exemple, les champs de vision des caméras à la seule surface nécessaire pour atteindre la ou les finalité(s) poursuivie(s), sans pour autant soumettre les salariés à une surveillance en permanence sur le lieu de travail.

Dans le même ordre d'idée, la Commission nationale siégeant en formation restreinte a retenu dans certaines de ses décisions que les champs de vision des caméras étaient disproportionnés et en violation dudit article 5.1.c) du RGPD, car ils permettaient de surveiller des terrains avoisinants ou la voie publique, alors qu'elle est d'avis que les caméras destinées à surveiller un lieu d'accès

(entrée et sortie, seuil, perron, porte, auvent, hall, etc.) doivent avoir un champ de vision limité à la surface strictement nécessaire pour visualiser les personnes s'apprêtant à y accéder. Les caméras qui filment des accès extérieurs ne doivent dès lors pas baliser toute la largeur d'un trottoir longeant, le cas échéant, le bâtiment ou les voies publiques adjacentes.

De même, les caméras extérieures installées aux abords ou alentours d'un bâtiment doivent être configurées de façon à ne pas capter la voie publique, ni les abords, entrées, accès et intérieurs d'autres bâtiments avoisinants rentrant éventuellement dans leur champ de vision.

Par ailleurs, 25 décisions étaient prises dans le cadre de **la campagne d'enquête thématique sur la fonction du délégué à la protection des données**. La CNPD a choisi au préalable 25 organismes, représentant les principaux secteurs d'activité et correspondant aux entités les plus importantes du pays en fonction du nombre d'employés, du nombre de traitements effectués et de la sensibilité des données traitées. L'objectif était de vérifier si les organismes choisis étaient en conformité avec les exigences du RGPD, en particulier avec les articles 37 à 39 du RGPD concernant la désignation du délégué à la protection des données, sa fonction et ses missions. Le plus souvent, la Commission nationale siégeant en formation restreinte a conclu dans ses décisions que l'article 38. 1 du RGPD n'a pas été respecté, car le délégué à la protection des données n'était pas associé de manière appropriée à toutes les questions relatives à la

4

LES ACTIVITÉS EN 2021

protection des données à caractère personnel ou que ledit délégué n'avait pas rempli ses missions d'information et de conseil, ainsi que sa mission de contrôle (article 39.1 a) et b du RGPD).

Quatre décisions de la Commission nationale siégeant en formation portaient **sur d'autres sujets**. Par exemple, dans une décision un manquement à l'obligation de documenter une violation de données à caractère personnel, de la notifier à la CNPD et de la communiquer à la personne concernée a été retenue (articles 33 et 34 du RGPD), tandis que dans une autre une non-conformité à l'article 15.2 de loi du 1^{er} août 2018 relative au traitement des données à caractère personnel en matière pénale et sécurité nationale (droit à l'effacement) a été constatée.

Un recours contre les décisions de la CNPD peut être ouvert devant le Tribunal administratif, qui statue sur le fond de l'affaire. Le délai de recours est de trois mois.

Toutefois, en application de l'article 42 de loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des

données et du régime général sur la protection des données, la CNPD est tenue au secret professionnel qui l'empêche de communiquer en détail sur un dossier spécifique.

En outre, en vertu de l'article 52 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la publication complète et en clair des décisions de la CNPD est à considérer comme une sanction supplémentaire.

Ledit article prévoit que la CNPD peut uniquement ordonner la publication de ses décisions si les voies de recours contre la décision sont épuisées et si la publication ne risque pas de causer un préjudice disproportionné aux parties en cause.

La CNPD publie par principe sur son site internet ses décisions de façon anonymisée et ceci même avant que les voies de recours ne soient épuisées, hormis les décisions pour lesquelles une publication anonyme n'est pas envisageable en raison de la qualité du responsable du traitement et du contenu de la décision.

LA PROCÉDURE RELATIVE AUX ENQUÊTES ET LA PRISE DE DÉCISION 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 1^{er} 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 sera entendu selon le principe du 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 1^{er} août 2018, c'est-à-dire d'ordonner la publication d'une décision de manière intégrale et nominative.

4

LES ACTIVITÉS EN 2021



LE CONTRÔLE DES TRAITEMENTS DE DONNÉES DES AUTORITÉS RÉPRESSIVES OU DE SÉCURITÉ NATIONALE

En application de la loi du 1^{er} 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 1^{er} 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 1^{er} 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.

1 Demandes d'information

La CNPD a traité 30 demandes d'information écrites ou orales en matière de traitement de données dans le domaine répressif et de sécurité nationale.

Environ un tiers des demandes d'informations concernaient les modalités de l'exercice du droit d'accès des personnes concernées en matière pénale eu égard aux spécificités des traitements de données mises en œuvre par les autorités répressives. Parmi les autres sujets en matière pénale ou de sécurité publique, les personnes

concernées et les responsables de traitement ont notamment sollicité la CNPD concernant la transmission de données à caractère personnel aux autorités compétentes dans le contexte de la recherche et la constatation d'infractions pénales. Finalement, la Commission nationale a répondu à des questions au sujet de l'utilisation du casier judiciaire dans les relations de travail.

Dans la continuité des travaux relatifs au « Fichier central » de la Police grand-ducale, la CNPD a participé à plusieurs réunions du groupe de suivi

4

LES ACTIVITÉS EN 2021

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. Des échanges ont également eu lieu avec l'Autorité nationale de sécurité et avec le Service de renseignement.

2 Avis

La CNPD a adopté 5 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 :

- les procédures de « contrôle d'honorabilité » (projet de loi n°7691) ;
- la Police grand-ducale (projet de loi n°7498) (2 avis) ;
- le fichier central de la Police grand-ducale (projet de loi n°7741) ;
- l'organisation des régimes internes des centres pénitentiaires.

L'avis concernant fichier central tenu par la Police grand-ducale 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>.

FICHER CENTRAL TENU PAR LA POLICE GRAND-DUCALE

La CNPD a rendu un avis sur le projet de loi n°7741 qui, selon ses auteurs, vise à adresser les critiques en matière de protection des

données qui ont été soulevées par rapport aux fichiers de la Police, et plus particulièrement par rapport au fichier central en été 2019. En effet, le ministre de la Sécurité intérieure avait sollicité la Commission nationale pour rendre un avis au sujet du fichier central et les recommandations émises à l'époque ont fait ressortir la nécessité d'un encadrement légal plus strict.

Dans son avis relatif au projet de loi n°7741, la CNPD a formulé des observations sur les modifications proposées concernant l'accès à des fichiers d'autres administrations par des agents de la Police grand-ducale, notamment en matière d'accès direct et indirect auxdits fichiers ou de la transmission manuelle de données par des administrations à la Police grand-ducale. Elle a également pris position sur les interactions entre le projet de loi et les dispositions légales existantes encadrant les fichiers d'autres administrations, et les finalités pour lesquelles un tel accès devrait pouvoir être utilisé, ainsi que les mesures à mettre en place relatives au contrôle des accès. La CNPD a ensuite analysé les dispositions relatives aux fichiers propres de la Police grand-ducale, en rappelant les exigences relatives à

l'encadrement législatif et réglementaire des traitements mis en œuvre par la Police grand-ducale. Elle a analysé les finalités proposées par le projet de loi pour les différents fichiers, dont principalement le fichier central, ainsi que les données visées par lesdits fichiers. Finalement, la CNPD s'est penchée sur le contrôle des accès et a analysé en détail les dispositions proposées en matière de durées de conservation des données dans le fichier central et les fichiers particuliers prévus par le projet de loi.

En conclusion, la CNPD a salué le projet de loi qui encadre de manière détaillée le fichier central. Elle a réitéré sa conviction que, dans le fonctionnement d'une société démocratique, il serait préférable d'encadrer par des dispositions légales ou réglementaires les traitements de données les plus intrusifs, de par le nombre de personnes concernées et de par la sensibilité des données traitées, mis en œuvre par la Police dans l'exercice de ses missions de police judiciaire ou de police administrative.

3 Réclamations

En 2021, la CNPD a été saisie d'une seule réclamation en matière pénale et de sécurité nationale. Une telle réclamation peut être introduite 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. En 2019, la CNPD avait reçu 11 réclamations dans ce domaine.

4 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.

Entre le 20 août 2018 (entrée en vigueur de la loi du 1^{er} 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 2021, la CNPD a reçu trois notifications de violations de données concernant des traitements de données à caractère personnel en matière pénale, ainsi qu'en matière de sécurité nationale.

4

LES ACTIVITÉS EN 2021

5 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. La CNPD a débuté les audits pour ces deux systèmes sur la deuxième moitié 2021.

6 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 biennuelles 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.

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.

4

LES ACTIVITÉS EN 2021



LA PROTECTION DE LA VIE PRIVÉE DANS LE SECTEUR DES COMMUNICATIONS ÉLECTRONIQUES

La Commission nationale est également chargée d'assurer l'application des dispositions de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de ses règlements d'exécution.

1 Violations de données dans le secteur des communications électroniques

Conformément au règlement (UE) No. 611/2013 de la Commission européenne du 24 juin 2013, les fournisseurs de services de communications électroniques accessibles au public, tels que les entreprises de téléphonie fixe/mobile ou les fournisseurs d'accès à Internet, doivent avertir la CNPD endéans les 24 heures suivant le constat d'une violation de sécurité et de confidentialité des données à caractère personnel. De surcroît, ils sont tenus d'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 2021, aucune violation de données dans le secteur des communications électroniques n'a été signalée à la CNPD.

4

LES ACTIVITÉS EN 2021

2 Rétention de données de trafic et de localisation

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

entre, d'une part, l'accès aux données traitées par des fournisseurs de communications électroniques dans le cadre de la lutte contre le terrorisme et la criminalité grave, et, d'autre part, la protection de la vie privée des citoyens.

Or, la directive a été annulée par la Cour de justice de l'Union européenne en date du 8 avril 2014 par l'arrêt « Digital Rights Ireland ». Les lois de transposition nationales n'ont toutefois pas été modifiées en conséquence et la Commission nationale n'a pas reçu d'instruction dans ce cadre par son ministère

de tutelle. Elle continue à lui transmettre annuellement en vue de leur continuation à la Commission européenne des statistiques sur la conservation des données au titre des articles 5 et 9. A cet effet, les fournisseurs de services ou opérateurs conservent et continuent à la Commission nationale, sur demande de celle-ci, les informations comprenant notamment :

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

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

En 2021, les autorités compétentes ont fait 2 541 demandes auprès des opérateurs. Ce chiffre a légèrement diminué (-15 %) par rapport à l'année 2020 où 2 990 demandes avaient été faites.

4

LES ACTIVITÉS EN 2021



LES 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 contribué en 2021 aux travaux de nombreux organismes 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.

- La Conférence de printemps avec son séminaire « European Case Handling Workshop ».

Comme en 2020 d'autre, d'autres réunions de travail et conférences 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 et
- la conférence des commissaires européens à la protection des données.

4

LES ACTIVITÉS EN 2021

1 European Data Protection Board (EDPB)



European Data Protection Board

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.

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 a organisé 15 réunions plénières dont une en présentiel rassemblant ses membres (en ce compris la CNPD), par rapport à 11 réunions plénières par année en moyenne depuis sa création.

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 12, ainsi qu'aux réunions biennuelles du Comité de Supervision Coordonnée (CSC).

Il s'agit des sous-groupes (« Expert Sub Groups») 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 Users;
- Key Provisions (KEYP);
- Strategic Advisory (SAESG);
- Social Media (SOCM);
- Technology (TECH).

La CNPD a assisté aux réunions de la Supplementary Measures Taskforce, de la 101 Complaints Taskforce et de la Cookie Taskforce.

L'autorité de contrôle luxembourgeoise a ainsi participé en 2021 à près de 200 réunions de groupes de travail sans compter les réunions en équipe de rédaction. 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 pour certains le rôle de rapporteur ou co-rapporteur.

L'année a été marquée par le suivi de nouvelles propositions législatives par la COM et l'encouragement et la facilitation de l'utilisation de l'ensemble des outils de coopération et de cohérence prévu dans le Chapitre VII du RGPD allant ainsi vers des actions coordonnées, un support pool d'experts et la mise en oeuvre d'une coopération transfrontalière uniforme et efficace. L'interprétation du guichet unique a été étoffée par le jugement dans l'affaire C-645/19 Facebook v Gegevensbeschermingsautoriteit par la Cour de Justice de l'UE du 15 juin 2021.

A côté de nombreux autres projets en cours, la CNPD a assumé le rôle du rapporteur et/ou co-rapporteur pour les projets suivants finalisés en 2021:

- Lettre à ENISA comprenant des recommandations quant au « EU cybersecurity certification Cloud Scheme » soumis à consultation publique;
- Version pour consultation publique de la guidance sur l'analyse des critères de certification (Addendum aux lignes directrices 1/2018 sur la certification et l'identification des critères de certification);
- Lignes directrices sur les assistants vocaux;
- Mise à jour de la procédure d'adoption des critères de certification.

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

- Lignes directrices sur les droits des personnes concernées;

4

LES ACTIVITÉS EN 2021

- Lignes directrices sur l'intérêt légitime ;
- Analyse des commentaires reçus lors de la consultation publique - Guidance sur l'analyse des critères de certification (Addendum aux lignes directrices 1/2018 sur la certification et l'identification des critères de certification).

Après avoir contribué en tant que lead-rapporteur à la mise en place de procédures pour l'adoption des critères d'agrément des organismes de certification, des critères de certification et d'un label européen pour la certification, la CNPD était en 2021 la première autorité à soumettre des critères de certification à l'EDPB pour avis.

DOCUMENTS ADOPTÉS EN 2021

L'EDPB a adopté de nombreux documents de travail, guidances et lettres.

- Recommandations 01/2021 sur les critères de référence pour l'adéquation dans le cadre de la directive en matière de protection des données dans le domaine répressif
- Lignes directrices 01/2021 sur les exemples de notification de violation de données
- Lignes directrices 02/2021 sur les assistants vocaux virtuels
- Recommandations 02/2021 sur la base juridique pour le stockage des données de carte de crédit dans le seul but de faciliter les transactions en ligne ultérieures
- Lignes directrices 03/2021 sur l'application de l'article 65, paragraphe 1, point a) du RGPD
- Lignes directrices 04/2021 sur les codes de conduite comme outils de transfert

- Lignes directrices 05/2021 sur l'interaction entre l'application de l'article 3 et les dispositions sur les virements internationaux conformément au chapitre V du RGPD
- Guidance sur l'analyse des critères de certification (Addendum aux lignes directrices 1/2018 sur la certification et l'identification des critères de certification)

Certains de ces documents sont résumés ci-dessous. Ils peuvent tous être téléchargés dans leur version complète sur Internet³.

Contribution à l'évaluation de la Directive (UE) 2016/680

L'EDPB et les différentes autorités de contrôle ont contribué à l'évaluation de la directive (UE) 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 la « Directive (UE) 2016/680 »), devant être réalisée par la Commission européenne conformément à l'article 62 de cette même directive. La CNPD a également contribué individuellement en fournissant des réponses à un questionnaire, accessible en ligne⁴. La contribution de l'EDPB⁵ se compose dès lors d'une synthèse des différentes réponses que les autorités de contrôles ont fourni au questionnaires ainsi que

³ https://edpb.europa.eu/our-work-tools/our-documents_fr

⁴ https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities-european-commissions-evaluation-led_en

⁵ https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-european-commissions-evaluation-data_en

de positions générales destinées aux acteurs politiques. Dans ces positions, l'EDPB soulève notamment qu'en raison de la transposition assez récente de la Directive (UE) 2016/680 par les Etats membres, et conséquemment de l'entrée en vigueur du régime applicable en matière de protection des données édicté par la Directive (UE) 2016/680, l'expérience et les statistiques des autorités de contrôle en relation avec les activités dans ce domaine sont limitées et en cours de développement. Par conséquent, l'EDPB est d'avis qu'il est trop tôt pour tirer des conclusions complètes sur l'efficacité de la Directive.

Première procédure de décision contraignante d'urgence conformément à l'article Art. 66 RGPD

L'EDPB a adopté sa première décision contraignante d'urgence à la suite d'une demande de l'autorité de contrôle de Hambourg, après que celle-ci ait adopté des mesures provisoires à l'encontre de Facebook Ireland Ltd (Facebook IE). Plus précisément, l'autorité de contrôle avait ordonné l'interdiction de traiter les données des utilisateurs de WhatsApp par Facebook IE pour ses propres besoins à la suite d'une modification des conditions de service et de la politique en matière de respect de la vie privée applicables aux utilisateurs européens de WhatsApp Ireland Ltd. L'EDPB a décidé qu'aucune mesure définitive ne devait être adoptée par l'autorité de contrôle irlandaise à l'encontre de Facebook IE dans ce cas, mais que l'autorité de contrôle devait procéder à une enquête réglementaire.

Déclarations et avis sur les nouvelles initiatives législatives

L'EDPB et le CEPD ont adopté un avis conjoint concernant la proposition relative à la proposition de Commission pour une réglementation sur la gouvernance des données (Data Governance Act, DGA). Ce règlement vise à favoriser la disponibilité de données en augmentant la confiance dans les intermédiaires de données et en renforçant les mécanismes de partage de données dans l'ensemble de l'UE. Notamment, elle est destinée à promouvoir la mise à disposition de données du secteur public en vue d'une réutilisation et le partage de données entre entreprises, tout en permettant l'utilisation de données à caractère personnel avec l'aide d'un « intermédiaire de partage de données à caractère personnel ». Cette proposition vise également à permettre l'utilisation de données pour des motifs altruistes.

Procédure de règlement de litige

Après l'examen par l'autorité irlandaise des objections formulées par les autorités concernées à l'encontre de son projet de décision à l'ensuite d'une enquête sur WhatsApp IE ouverte de sa propre initiative, une procédure de règlement de litige a été initiée. La décision de l'EDPB porte sur le fond des objections jugées « pertinentes et motivées » visant à déterminer si WhatsApp IE respectait ou non les obligations en matière de transparence qui lui incombent.

4

LES ACTIVITÉS EN 2021

Adoption de la décision d'adéquation pour la Corée du Sud

Le Comité européen de la protection des données s'est concentré sur les aspects généraux du RGPD et l'accès des autorités publiques aux données à caractère personnel transférées de l'Espace économique européen (EEE) à la République de Corée à des fins répressives et de sécurité nationale, y compris les voies de recours disponibles pour les particuliers au sein de l'EEE et le caractère effectif de l'application des garanties prévues par le cadre juridique coréen.

En tenant compte de l'avis délivré par l'EDPB, la Commission européenne a constaté le 17 décembre 2021, dans sa décision d'adéquation que la République de Corée assure un niveau de protection adéquat en matière de protection des données à caractère personnel, conformément au règlement général sur la protection des données.

Lancement de la première action coordonnée

L'EDPB a voté le cadre pour les actions coordonnées, le « Coordinated Enforcement Framework » (CEF) en 2020. Il a maintenant été décidé de lancer la première action coordonnée sur l'utilisation par le secteur public des services basés sur le Cloud. Dans une action coordonnée, l'EDPB donne la priorité à un certain sujet sur lequel les autorités membres peuvent travailler au niveau national.

Plan de projet pour le support pool d'experts (SPE)

En poursuivant les actions clés de la stratégie EDPB 2021-2023, l'EDPB s'est mis d'accord sur le plan de projet du SPE. Le SPE vise à fournir un soutien matériel aux membres de l'EDPB sous la forme d'une expertise utile pour les enquêtes et les activités d'exécution et à renforcer la coopération et la solidarité entre les membres de l'EDPB en partageant, renforçant et complétant leurs forces et en répondant aux besoins opérationnels.

Avis relatif à la cohérence

Afin de garantir l'application cohérente du RGPD dans les affaires ayant des implications transfrontières, l'EDPB a émis 30 avis relatifs à la cohérence.

2 Conférence internationale de la 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. Créée en 1979, elle était connue sous le nom de « International Conference of Data Protection and Privacy Commissioners (ICDPPC) » jusqu'en 2019.

La CNPD a participé aux sessions ouvertes et fermées de la 43^e édition de la réunion globale sur la vie privée, organisée en ligne du 18 au 21 octobre 2021.

Les discussions entre les commissaires et autres parties prenantes ont porté sur des enjeux importants en la matière, comme notamment la reconnaissance faciale, Big Data, les traitements des données dans le cadre du Covid-19, les transferts internationaux de données, l'Internet des Objets, l'intelligence artificielle, smart cities ou encore l'identité numérique.

La session à huis clos a été ouverte par Elizabeth Denham, présidente sortante du GPA et commissaire britannique à l'information. Elle a salué le travail de la communauté de la protection de la vie privée pendant la pandémie, appelant à ce que l'Assemblée continue à avoir un impact.

Mme Denham a déclaré : « *Nous étions déjà dans une ère axée sur les données, avant même que la pandémie n'amplifie cette accélération de la croissance numérique. Aujourd'hui, l'innovation basée sur les données nous aide à traverser les crises sanitaires et influence toutes les facettes de la société.*

Le travail de notre communauté est au cœur de cela, garantissant que les gens font confiance à cette innovation. Mais nous ne pouvons pas supposer que la vie privée aura toujours une place à la table. Notre contribution aux discussions sur les principaux problèmes de société dépend de la compréhension que les superviseurs de la protection des données et de la confidentialité apportent un aperçu précieux, un état d'esprit pratique et que nous pouvons répondre rapidement. »

Des résolutions ont été discutées et approuvées lors de la conférence, donnant un point de vue partagé sur une gamme de sujets d'actualité importants :

4

LES ACTIVITÉS EN 2021

- partage de données pour le bien public ;
- les droits numériques des enfants ;
- accès du gouvernement aux données ;
- l'avenir de la Global Privacy Assembly ;
- la coopération internationale en matière d'application de la loi ;
- et les bacs à sable réglementaires.

L'Assemblée a également adopté un plan stratégique pour les deux prochaines années, s'engageant à continuer à se concentrer sur la promotion de la confidentialité mondiale, à maximiser l'influence de la GPA et à renforcer les capacités des membres.

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.

Conformément à ces objectifs, la CNIL et la CNPD, en tant que co-responsables du groupe de travail, ont continué à actualiser et à réorganiser

la plate-forme de ressources CIRCABC afin de mettre à jour et d'améliorer la qualité des ressources de la bibliothèque en ligne tout en respectant une nouvelle classification par types de supports d'enseignement et de formation, y ajoutant des rubriques complémentaires pour répondre aux attentes actuelles. Ce travail de mise à jour a été accompli jusqu'en décembre 2020 avec la CNPD intervenant au niveau de la gestion technique pour téléchargement des documents modifiés par les membres de la GPA au sein de la nouvelle architecture de classement et la suppression des documents jugés plus pertinents.

Le nouveau tableau qui répertorie les 137 ressources actualisées a été diffusé à la fin du mois de février 2021. Il s'agit notamment d'outils d'apprentissage interactifs, plans de cours/scénarios, guides, mémos, FAQ, mesures de sécurité, vidéos et conseils sur la protection de votre vie privée, bandes dessinées, jeux en ligne, destinées aux différents publics, à savoir les enseignants et le personnel éducatif, les parents, les enfants et les jeunes par groupes d'âge.

Pour accélérer le renouvellement de la bibliothèque en ligne en lien avec les thématiques prioritaires, et pour familiariser les nouveaux utilisateurs avec la plateforme, un tutoriel vidéo de formation spécifique, en anglais sous-titré en français, a été conçu et une présentation PowerPoint adaptée a été mise à disposition.

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

En raison de l'épidémie du COVID-19, la Conférence des autorités européennes de protection des données 2021 a dû être reporté.

Les préparations de la Conférence pour l'année 2022 en Croatie ont été reprises.

4 Le séminaire « European Case Handling Workshop »

Le séminaire « European Case Handling Workshop » a eu lieu le 16-17 novembre 2021 en ligne, organisé par l'autorité de contrôle de Gibraltar. Le séminaire a porté sur des thématiques intéressant notamment les

gestionnaires de dossiers des autorités de contrôle et consiste dans des échanges interactifs sur la gestion des réclamations, la conduite d'investigations et les politiques de sanctions.



RESSOURCES, STRUCTURES
ET FONCTIONNEMENT

5

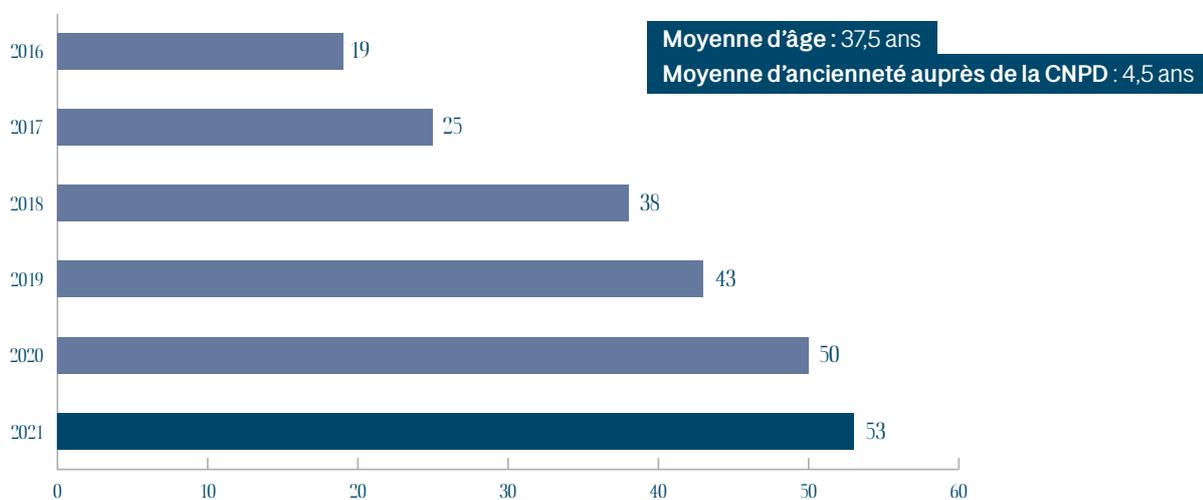


5

RESSOURCES, STRUCTURES ET FONCTIONNEMENT



1 Ressources humaines



COLLÈGE

Tine A. LARSEN,
Présidente

Thierry LALLEMANG,
Commissaire

Marc LEMMER,
Commissaire

Alain HERRMANN,
Commissaire
(a remplacé Christophe BUSCHMANN
le 1^{er} septembre 2021)

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

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

Kathrin KRAEMER,
Juriste, Secrétaire adjointe du Collège
« Formations 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,
Licencié et Maître en Informatique

François THILL,
Ministère de l'Économie,
Directeur du commerce électronique
et de la sécurité de l'information

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

Cristina FERNANDES DA CUNHA,
Rédacteur, 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

DATA PROTECTION OFFICER

Bertrand NAVARRE,
Juriste, Délégué à la protection des données

RELATIONS 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 »

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 »

5

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

Carmen SCHANCK,
Chef d'unité « Avis juridiques »

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

Nina BURMEISTER,
Juriste, Demandes d'informations

Regina DECOVILLE,
Juriste, Demandes d'informations

Céline DEROOSE,
Juriste, Demandes d'informations

Marie DOUZAL,
Juriste, Avis juridiques

Kalliroy GRAMMENO,
Juriste, Transferts pays tiers

Christian WELTER,
Juriste, Demandes d'informations

SERVICE CONFORMITÉ

Alain HERRMANN,
Commissaire

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

Elena-Cristina GERTH,
Auditeur

SERVICE RÉCLAMATIONS

Thierry LALLEMANG,
Commissaire

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

Georges WEILAND,
Chef d'unité « Réclamations européennes »

Sabrine ABAAB,
Juriste, Réclamations européennes

Jessica BLEEK,
Juriste, Réclamations européennes

Gaël DUMORTIER,
Juriste, Réclamations nationales

Diana FERREIRA,
Juriste, Réclamations nationales

Barbara GIROUD,
Juriste, Réclamations nationales

Aleksandra GUCWA,
Juriste, Réclamations internationales

Nicolas RASE,
Juriste, Réclamations nationales

SERVICE ENQUÊTES

Alain HERRMANN,
Commissaire

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

Edith MALHIÈRE,
Chef d'unité « Audits »

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

5

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

NOMINATION DE ALAIN HERRMANN EN TANT QUE COMMISSAIRE

En date du 27 août 2021, Monsieur Alain Herrmann a été assermenté en tant que Commissaire à la protection des données auprès de la CNPD.

Alain Herrmann est fonctionnaire auprès de la CNPD depuis 2012. Il y a débuté en tant qu'expert en informatique et nouvelles technologies pour évoluer jusqu'au poste de chef du service Conformité.

Auparavant, il a été actif pendant plus de 14 ans comme ingénieur et consultant en sécurité IT / sécurité de l'information auprès de diverses organisations privées.

Alain Herrmann dispose d'une connaissance excellente de l'écosystème national, européen et international de la protection des données.

Son expérience et sa propension à sortir de sa zone de confort permettra à la CNPD de continuer son développement pour faire face aux défis à venir et d'assurer la continuité des activités de la CNPD à partir du 1er septembre 2021.



ASSERMENTATIONS AUPRÈS DE LA CNPD

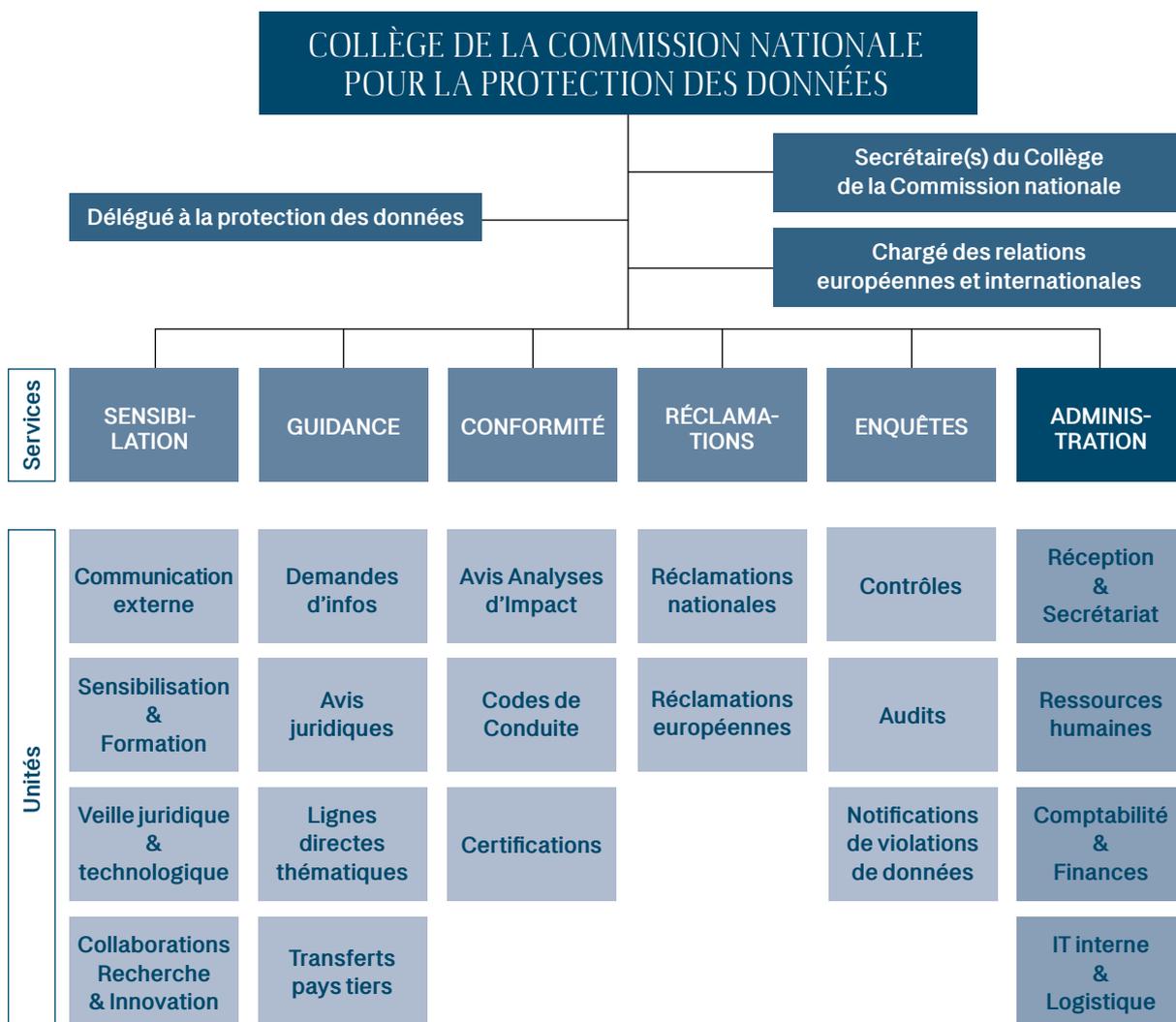
En 2021, Madame Tine A. Larsen, Présidente de la CNPD, a procédé à l'assermentation de 5 nouveaux agents en tant que fonctionnaire :

- Anna Magi (assermentée en date du 27 janvier 2021 et nommée à la fonction de rédacteur)
- Christine Andres (assermentée en date du 28 avril 2021 et nommée à la fonction de chargé d'études)
- Arnaud Habran (assermenté en date du 28 avril 2021 et nommé à la fonction d'attaché)
- Florent Kling (assermenté en date 27 août 2021 et nommé à la fonction d'attaché)
- Cristina Fernandes (assermentée en date 1^{er} octobre 2021 et nommée à la fonction de rédacteur)

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 1^{er} janvier 2020.



5

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

3 Rapport de gestion relatif aux comptes de l'exercice 2021

La Commission nationale pour la protection des données (CNPD) avait adopté en mai 2020 un document intitulé « Stratégie et programme de travail 2020-2022 » lui permettant de mieux planifier, coordonner et suivre ses activités pendant la période afférente et d'améliorer ainsi la gestion de ses ressources.

Un nouvel organigramme établi sur base des expériences collectées lors de la première année sous le régime du RGPD et adopté par le Collège de la CNPD en janvier 2020, prévoyait en outre un renforcement du personnel visant à atteindre 62 postes à plein temps à partir de 2023. Or, au vu de la réduction de la dotation attribuée à la CNPD pour l'exercice 2021 et suivants, les recrutements ainsi prévus ont dû être reportés, l'effectif total autorisé pour 2021 restant dès lors au niveau atteint en 2020, à savoir 54 équivalents temps-plein.

Se situant en plein milieu de la période de référence visé par le document mentionné en amont, l'année 2020 a bien sûr été marquée par

la pandémie de Covid-19 et ses répercussions non négligeables sur les activités de la CNPD, mais surtout par le prononcé en juillet 2021, des premières décisions prises en vertu de l'article 41 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, dont certaines assorties de sanctions financières.

Concernant les dépenses de l'exercice 2021, il y a lieu de noter que certains chiffres ne sauraient être considérés comme représentatifs en raison notamment de la crise sanitaire et des mesures qui en découlent.

Si la crise sanitaire a eu pour conséquence une diminution de certaines catégories de dépenses, les honoraires juridiques en rapport avec les sanctions prononcées par la CNPD ont, de leur côté, généré des dépenses supplémentaires considérables.

LE BUDGET

Le budget de la CNPD s'est élevé pour l'exercice 2021 à un montant de 7.200.000 €, soit une diminution de 6 % par rapport au budget de de l'année précédente. La réduction de 467.224 € par rapport à 2020 résulte principalement du fait que les prévisions budgétaires se rapportant aux frais de personnel, fournies lors de l'élaboration du budget 2021 par le Centre de gestion du personnel et de l'organisation de l'Etat (CGPO), se situaient largement en dessous des frais auxquels il fallait s'attendre.

LES DÉPENSES

Au cours de l'exercice 2021, le total des dépenses de l'établissement public s'est élevé à 7.472.869 € par rapport à 6.336.137 € en 2020, soit une augmentation de 18 %, dépassant ainsi de 272.869€ les dépenses prévues au budget.

Le dépassement des crédits accordés et qui n'est pas à confondre avec le résultat d'exploitation négatif au montant de 224.517 €, provient essentiellement des honoraires juridiques en relation avec les recours introduits contre des sanctions financières infligées par la CNPD dans le cadre de trois de ses décisions prononcées en 2021.

5

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

1. ACTIF IMMOBILISÉ

Dans le respect de l'article 46 de la loi du 1^{er} 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 2021, le mobilier supplémentaire nécessaire dans le cadre de l'aménagement des nouveaux bureaux a engendré une dépense de 10.410 €, par rapport à 70.644 € en 2020.

Les dépenses en vue de l'acquisition de nouveaux équipements informatiques se sont élevées à 4.405 €, alors qu'en 2020 et compte tenu des engagements de renforcement réalisés les frais afférents étaient de 21.681 €.

2. FRAIS DE FONCTIONNEMENT

Les frais de fonctionnement se sont élevés à 1.188.318 € par rapport à 806.279 € en 2020, soit une augmentation de 382.039 € respectivement 47 %, dépassant ainsi les prévisions budgétaires initiale au montant de 994.048 €.

2.1. Frais généraux

La progression précitée provient essentiellement des frais d'honoraires, et plus particulièrement des honoraires juridiques inexistant en 2020.

En effet, et mis à part le loyer et les charges locatives au montant de 611.163 €, les frais d'honoraires juridiques s'élevant à 284.876 €, représentent la part la plus importante des frais généraux. Il s'agit en l'occurrence des frais se rapportant aux trois recours introduits contre des décisions assorties de sanctions financières prononcées par la CNPD en 2021.

S'y ajoutent encore les frais d'entretien des locaux de la CNPD au montant de 87.390 € par rapport à 42.335 € en 2020, frais qui à l'époque et compte tenu du déménagement en juin en 2020, ne couvraient en fait que six mois.

Les dépenses se rapportant aux équipements et fournitures de bureau, les frais de documentation, de même que les frais de port et de télécommunication s'élevant à respectivement 14.975 €, 6.869 € et 10.934 € sont restés au même niveau qu'en 2020.

Quant aux frais d'honoraires, ils comprennent outre les honoraires juridiques mentionnés en amont, les dépenses relatives à la tenue des livres comptables se chiffrant à 5.850 € ainsi qu'à la révision des comptes dont les frais se sont élevés à 5.910 €.

Les autres charges générales d'exploitation au montant de 22.593 €, comprenant notamment les frais d'assurance, d'électricité ainsi que de gardiennage se chiffrant à respectivement 10.758 €, 4.579 € et 4.558 €, sont restées stables, et ce compte tenu des frais de déménagement de 30.448 € compris dans le solde de compte en 2020.

2.2. Communication et relations publiques

Comme suite à la crise sanitaire, toutes les réunions et conférences à l'étranger ont été systématiquement remplacées par des vidéo-conférences de sorte que les frais de voyage, de représentation et de relations publiques au montant de 2.751 € sont restés largement en dessous tant des prévisions budgétaires se chiffrant à 52.000 € que des dépenses engendrées en 2020 et s'élevant à 9.002 €.

Les frais de communication et de publication sont restés stables par rapport à 2020, tout en se limitant aux frais de publication du Rapport annuel 2020 s'élevant à 9.146 € ainsi qu'aux annonces et insertions se chiffrant à 8.030 €, auxquels s'ajoutent divers autres achats de services publicitaires au montant de 4.771 €.

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 tout comme pour l'exercice 2020 ont été réduites à zéro.

2.3. Frais informatiques

Les frais informatiques se sont élevés en 2021 à 117.465 € par rapport à 63.261 en 2020 tout en restant en dessous du crédit budgétaire accordé au montant de 156.293 €. Cette variation résulte d'abord de la redevance due à partir de 2021 au Centre des technologies de l'information de l'État pour la mise à disposition des licences informatiques, des appareils téléphoniques et autre matériel, et dont les frais afférents se sont élevés à 88.540 €.

Or, cette augmentation considérable a pu être atténuée en raison de la résiliation de commun accord du contrat conclu avec la société « eProceed », société qui hébergeait 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. Les frais afférents se sont élevés en 2020 à 54.405 € et n'étaient dès lors plus dus pour l'année 2021.

Pour ce qui est de la maintenance des équipements et des autres frais informatiques, il est à noter que les dépenses afférentes sont restées stables par rapport à celles de l'exercice 2020.

5

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

3. FRAIS DE PERSONNEL

Les rémunérations du personnel se sont élevées en 2021 à 6.199.267 € par rapport à 5.387.440 € en 2020. Cette progression est due au renforcement du personnel réalisé mi et fin 2020 et au courant de 2021.

Malgré une augmentation considérable des effectifs relevée en fin d'année et en dépit du fait que les estimations réalisées par le CGPO se situaient largement en dessous des frais auxquels il fallait s'attendre, les dépenses effectives n'ont dépassées les prévisions budgétaires que d'un montant de 51.889 €, ceci en raison du fait que le recrutement de six agent supplémentaires a été échelonné sur toute l'année 2021.

Outre les quatre commissaires, le cadre du personnel permanent comprenait au 31 décembre 2021 :

- 43 agents du groupe de traitement ou d'indemnité A1 dont 15 fonctionnaires,
- 1 employé du groupe d'indemnité A2 ainsi que
- 5 agents du groupe de traitement ou d'indemnité B1 dont 4 fonctionnaires.

Mises à part les rémunérations, les frais de personnel comprennent encore un montant de 19.239 € représentant les dépenses se rapportant à la formation du personnel. La progression par rapport à 2020 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 6.478 € par rapport à 4.242 € en 2020. Cette variation résulte d'un recalcul en faveur de la CNPD du loyer mensuel suite à une renégociation avec effet rétroactif du contrat de leasing basé sur les distances effectivement parcourues. Il s'ensuit qu'en 2020, le solde de ce poste comprenait un montant de 2.487 €, remboursé à la CNPD suite à ladite renégociation.

L'amortissement du mobilier et du matériel informatique comptabilisé pour un montant de 44.024 € suit celui des investissements effectués et représente une augmentation de 16 % par rapport à 37.993 € pour l'exercice 2020.

S'y ajoutent encore les frais bancaires et charges assimilées au montant de à 609 €.

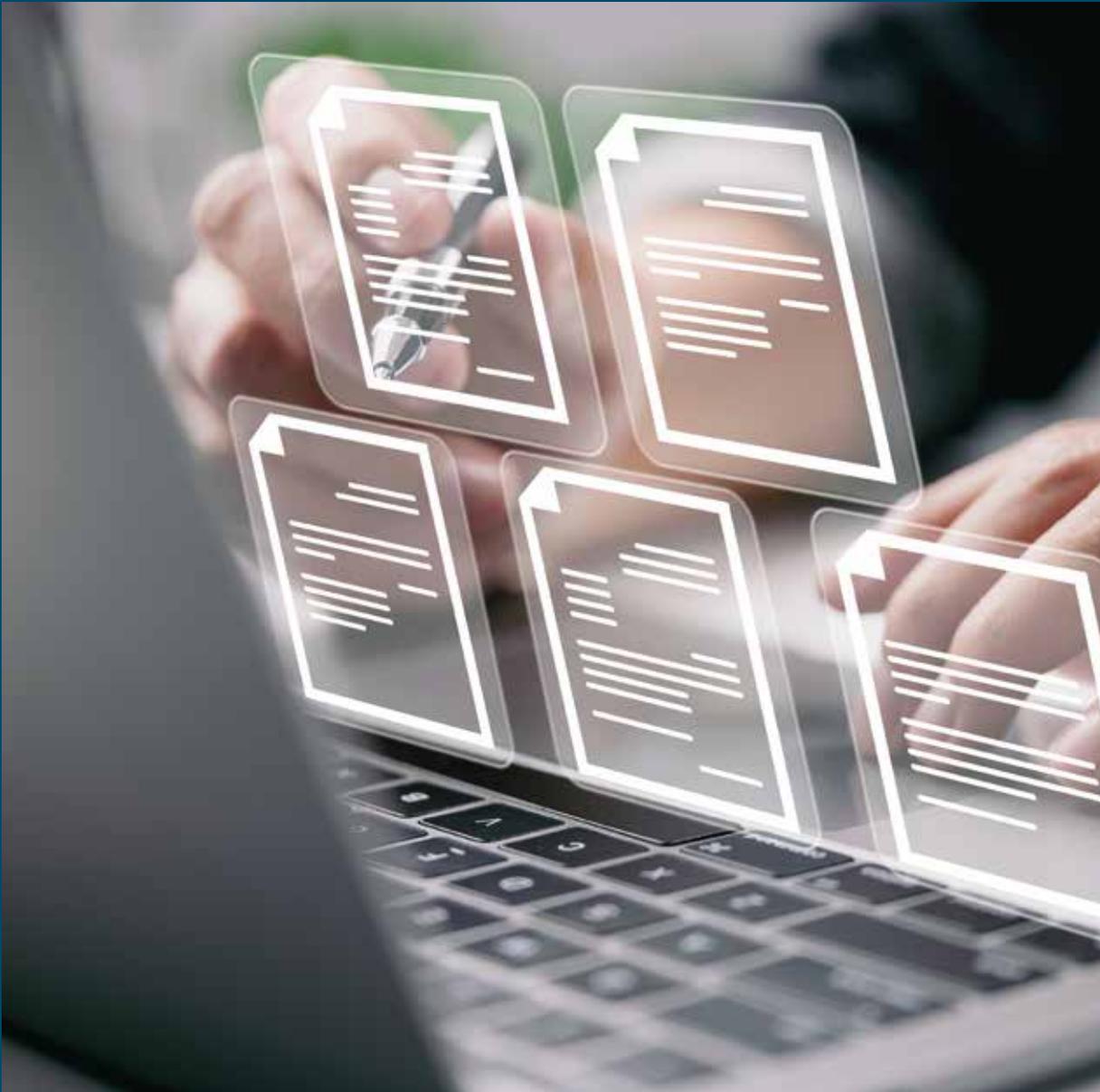
LES RECETTES

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 1^{er} 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.

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 32.538 €. S'y ajoute encore un montant de 1.000 € perçu en application de l'article 3 du Règlement N°7/2020 du 3 avril 2020 de la Commission nationale pour la protection des données fixant le montant et les modalités de paiement des redevances dans le cadre de ses pouvoirs d'autorisation et de consultation, pour l'analyse d'une demande d'agrément préalable.

LE RÉSULTAT D'EXPLOITATION

Compte tenu de la dotation annuelle de 7.200.000 €, dont la Commission nationale pour la protection des données a bénéficié de la part de l'Etat en application de l'article 47 de la loi du 1^{er} août 2018 précitée, le résultat d'exploitation négatif de l'établissement public s'élève au 31 décembre 2021 à 224.517 €.



ANNEXES

6



6

ANNEXES

Les annexes peuvent être téléchargées sur le site de la CNPD à l'adresse <https://cnpd.public.lu/fr/publications/rapports/index.html>

AVIS ET DÉCISIONS

P117

- Avis relatif au projet de loi n°7643 sur **les données ouvertes et la réutilisation des informations du secteur public** et relatif au projet de règlement grand-ducal portant fixation de critères objectifs, transparents et vérifiables pour calculer le montant total des redevances pour la fourniture et les autorisations de réutilisation des documents détenus par les organismes du secteur public et les entreprises publiques. (Délibération n°1/2021 du 20/01/2021)

P125

- Avis complémentaire relatif au projet de loi n°7425 portant : 1° transposition de la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du Conseil relative au **contrôle de l'acquisition et de la détention d'armes** ; 2° modification du Code pénal, et 3° abrogation de la loi du 20 avril 1881 concernant le transport et le commerce des matières explosives. (Délibération n°2/2021 du 4/02/2021)

P152

- Avis relatif au projet de loi n°7691 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.
(Délibération n°3/AV3/2021 du 10/02/2021)

P188

- Avis relatif au projet de loi n°7768 portant modification de la loi modifiée du 17 juillet 2020 sur **les mesures de lutte contre la pandémie Covid-19**.
(Délibération n°5/AV4/2021 du 16/02/2021)

P195

- Avis relatif au projet de règlement grand-ducal relatif à la **détermination et à l'organisation des formations des cadres techniques et administratifs pour les différentes formes d'activités sportives**.
(Délibération n°6/AV5/2021 du 24/02/2021)

P199

- Avis relatif au projet de loi n°7632 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 **établissant le code des communications électroniques européen** et portant modification de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut Luxembourgeois de Régulation ; 2) modification de la loi modifiée du 22 juin

1963 fixant le régime des traitements des fonctionnaires de l'Etat.

(Délibération n°7/AV6/2021 du 03/03/2021)

P208

- Deuxième 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°8/AV7/2021 du 3/03/2021)

P215

- Avis relatif au projet de loi n°7751 modifiant 1° le **Code de la sécurité sociale** ; 2° le Code du travail ; 3° la loi modifiée du 15 décembre 1993 déterminant le cadre du personnel des administrations, des services et des juridictions de la sécurité sociale; et 4° la loi modifiée du 28 juillet 2000 ayant pour objet la coordination des régimes légaux de pension.
(Délibération n°9/AV8/2021 du 03/03/2021)

P218

- Avis relatif au projet de loi n°7784 portant modification de la loi modifiée du 17 juillet 2020 sur les **mesures de lutte contre la pandémie Covid-19**.
(Délibération n°10/AV9/2021 du 8/03/2021)

P220

- Avis relatif au projet de loi n°7741 portant modification 1° de la loi modifiée du 18 juillet 2018 sur la **Police grand-ducale** ; 2° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 3° du Code pénal.
(Délibération n°10/AV10/2021 du 16/03/2021)

6

ANNEXES

P260

- Avis relatif au projet de loi n°7795 portant modification de la loi modifiée du 17 juillet 2020 sur les **mesures de lutte contre la pandémie Covid-19**.
(Délibération n°14/AV11/2021 du 29/03/2021)

P266

- Troisième 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°16/AV12/2021 du 28 avril 2021)

P271

- Avis relatif à l'avant-projet de règlement grand-ducal relatif à la **composition et au fonctionnement de la commission consultative pour l'évaluation de la vidéosurveillance**.
(Délibération n°17/AV13/2021 du 7/05/2021)

P273

- Avis relatif au projet de loi n°7763 1. portant **introduction d'un fonds de travaux** ; 2. modifiant la loi modifiée du 16 mai 1975 portant statut de la copropriété des immeubles bâtis et au projet de règlement grand-ducal modifiant le règlement grand-ducal prescrivant les mesures d'exécution de la loi du 16 mai 1975 portant statut de la copropriété des immeubles.
(Délibération n°18/AV14/2021 du 14/05/2021)

P275

- Avis relatif au projet de loi n°7787 relatif à la mise en œuvre du règlement (UE) 2017/821 du Parlement européen et du Conseil du

17 mai 2017 fixant des **obligations liées au devoir de diligence à l'égard de la chaîne d'approvisionnement pour les importateurs de l'Union qui importent de l'étain, du tantale et du tungstène, leurs minerais et de l'or provenant de zones de conflit ou à haut risque**.

(Délibération n°19/AV15/2021 du 14/05/2021)

P277

- Avis relatif à la proposition de loi n°7808 relative à la **stratégie de dépistage du virus Covid-19 dans les structures pour personnes vulnérables et dans les réseaux d'aides et de soins**.
(Délibération n°20/AV16/2021 du 28/05/2021)

P281

- Avis relatif à la proposition de loi n°7797 portant modification de la loi modifiée du 17 juillet 2020 sur les **mesures de lutte contre la pandémie Covid-19**.
(Délibération n°21/AV17/2021 du 28/05/2021)

P282

- Avis relatif au projet de règlement grand-ducal prescrivant un **recensement général de la population, des logements et des bâtiments du Grand-Duché** au 1^{er} juin 2021 et amendements gouvernementaux.
(Délibération n°23/AV18/2021 du 1^{er} juin 2021)

P300

- Avis relatif au projet de loi n°7836 portant modification de la loi modifiée du 17 juillet 2020 sur les **mesures de lutte contre la pandémie Covid-19**.
(Délibération n°24/AV19/2021 du 8 juin 2021)

P302

- Avis complémentaire relatif au projet de règlement grand-ducal prescrivant un **recensement général de la population, des logements et des bâtiments du Grand-Duché** au 8 novembre 2021.
(Délibération n°25/AV20/2021 du 2/07/2021)

P307

- Avis complémentaire relative aux amendements gouvernementaux au projet de loi n°7126 relatif aux **sanctions administratives communales et à l'élargissement des compétences des agents municipaux**.
(Délibération n°26/AV21/2021 du 9 juillet 2021)

P310

- Avis complémentaire relatif au projet de loi n°7348 relative aux **comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence** et modifiant : 1. la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et 2. la loi modifiée du 7 décembre 2015 sur le secteur des assurances.
(Délibération n°27/AV22/2021 du 6 août 2021)

P312

- Avis complémentaire relatif à l'amendement parlementaire au projet de loi n°7643 **sur les données ouvertes et la réutilisation des informations du secteur public** et relatif au projet de règlement grand-ducal portant fixation de critères objectifs, transparents et vérifiables pour calculer le montant total des redevances pour la fourniture et les autorisations de réutilisation des documents détenus par les organismes du secteur public

et les entreprises publiques.

(Délibération n°28/AV23/2021 du 6/08/2021)

P314

- Deuxième avis complémentaire relatif au projet de loi n°7425 sur **les armes et munitions** et portant : 1° transposition de la directive (UE) 2021/555 du Parlement européen et du Conseil du 24 mars 2021 relative au contrôle de l'acquisition et de la détention d'armes ; 2° modification du Code pénal, et 3° abrogation de la loi du 20 avril 1881 concernant le transport et le commerce des matières explosives.
(Délibération n°29/AV24/2021 du 1^{er} octobre 2021)

P320

- Avis relatif au projet de loi n°7818 portant modification du **Code de la consommation** aux fins de transposition de 1. la directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques ; 2. la directive (UE) 2019/771 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens, modifiant le règlement (UE) 2017/2394 et la directive 2009/22/CE et abrogeant la directive 1999/44/CE.
(Délibération n°30/AV25/2021 du 1/10/2021)

P328

- Avis relatif au projet de loi n°7762 modifiant la loi du 5 juillet 2016 portant **organisation des services de taxis**.
(Délibération n°31/AV26/2021 du 1/10/2021)

6

ANNEXES

P339

- Avis relatif au projet de règlement grand-ducal portant **organisation des régimes internes des centres pénitentiaires**.
(Délibération n°32/AV27/2021 du 1/10/2021)

P352

- Avis relatif au projet de loi n°7897 portant modification: 1° de la loi modifiée du 17 juillet 2020 sur les **mesures de lutte contre la pandémie Covid-19** ; 2° de la loi modifiée du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière ; 3° de la loi modifiée du 22 janvier 2021 portant : 1° modification des articles L. 234-51, L. 234-52 et L. 234-53 du Code du travail ; 2° dérogation temporaire aux dispositions des articles L. 234-51, L. 234-52 et L. 234-53 du Code du travail.
(Délibération n°34/AV28/2021 du 12/10/2021)

P356

- Avis relatif aux amendements à la proposition de **révision du chapitre II de la Constitution** (numéro de dossier parlementaire : 7755)
(Délibération n°48/AV29/2021 du 29/10/2021)

P360

- Avis relatif au projet de loi n°7674 portant organisation de l'accès à la **connaissance de ses origines** dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs.
(Délibération n°52/AV30/2021 du 29/11/2021)

P382

- Avis relatif au projet de loi n°7924 portant modification de la loi modifiée du 17 juillet 2020 sur les **mesures de lutte contre la pandémie Covid-19**.
(Délibération n°53/AV31/2021 du 8/10/2021)

P389

- Avis complémentaire relatif au projet de loi n°7924 portant modification de la loi modifiée du 17 juillet 2020 sur les **mesures de lutte contre la pandémie Covid-19**.
(Délibération n°54/AV32/2021 du 10 décembre 2021)

P396

- Avis relatif au projet de loi n°7805 portant **création d'une carte de stationnement pour personnes handicapées** et relatif au projet de règlement grand-ducal 1° fixant le modèle et le contenu de la carte de stationnement pour personnes handicapées ainsi que la demande et du certificat médical en vue de l'obtention de cette carte ; 2° modifiant le règlement grand-ducal modifié du 26 août 1993 relatif aux avertissements taxés, aux consignations pour contrevenants non-résidents ainsi qu'aux mesures d'exécution de la législation en matière de mise en fourrière des véhicules et en matière de permis à points.
(Délibération n°55/AV33/2021 du 10 décembre 2021)

Conformément à l'article 57, paragraphe 1^{er}, 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 (ci-après le « règlement général sur la protection des données » ou le « RGPD »), auquel se réfère l'article 7 de la loi du 1^{er} 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 13 juillet 2020, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer sur projet de loi n°7643 sur les données ouvertes et la réutilisation des informations du secteur public (ci-après le « projet de loi »). Par courrier en date du 15 juillet 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 de critères objectifs, transparents et vérifiables pour calculer le montant total des redevances pour la fourniture et les autorisations de réutilisation des documents détenus par les organismes du secteur public et les entreprises

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7643 sur les données ouvertes et la réutilisation des informations du secteur public et relatif au projet de règlement grand-ducal portant fixation de critères objectifs, transparents et vérifiables pour calculer le montant total des redevances pour la fourniture et les autorisations de réutilisation des documents détenus par les organismes du secteur public et les entreprises publiques. (Délibération n°1/2021 du 20/01/2021)

publiques (ci-après le « projet de règlement grand-ducal »).

Le projet de loi a pour objet de transposer en droit national la directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte) (ci-après la « directive ») ainsi que d'abroger et remplacer la loi modifiée du 4 décembre 2007 sur la réutilisation des informations du secteur public.

Le projet de règlement grand-ducal a pour objet d'exécuter les dispositions de l'article 7, paragraphe 3, du projet de loi. Il détermine les critères objectifs, transparents et vérifiables pour calculer le montant total des redevances applicables par les organismes du secteur public tenus, en vertu du projet de loi, de générer des recettes destinées à couvrir une part substantielle des coûts liés à l'accomplissement de leurs missions de service public ainsi que les entreprises publiques, telles que définies à l'article 2, point 3, du projet de loi.

La CNPD entend limiter ses observations au regard des situations où des documents ou

6

ANNEXES

informations publiques mis à disposition à des fins de réutilisation qui comporteraient des données à caractère personnel au sens de l'article 4, paragraphe 1, du RGPD.

La Commission nationale note avec intérêt l'extension du champ d'application à l'égard des « données ouvertes et de réutilisation des informations du secteur public » par l'article 1^{er}, paragraphe (1), du projet de loi. La CNPD rappelle à cet égard le considérant 154 du RGPD qui énonce que l'« accès du public aux documents officiels peut être considéré comme étant dans l'intérêt public ». La Commission nationale ne peut que souscrire aux objectifs poursuivis par cette initiative législative qui concourt à rendre plus effectif le droit pour les citoyens de s'informer des affaires publiques. Dans le même temps, elle se soucie de parvenir à la définition d'un cadre juridique où la réutilisation des données publiques et la protection de la vie privée et des données à caractère personnel trouvent un équilibre. Il lui importe que la protection des données contribue à construire un cadre juridique solide et exigeant pour une meilleure transparence de l'action publique.

Il ressort du considérant 23 de la directive que celle-ci « fait obligation aux États membres de rendre tous les documents existants réutilisables, à moins que des règles nationales relatives à l'accès aux documents ne limitent ou n'excluent cet accès ou sous réserve des autres exceptions prévues par la présente directive » et qu'elle « s'appuie sur les règles d'accès en vigueur dans les États membres et ne modifie

pas les règles nationales en matière d'accès aux documents. »

Le considérant 52 de la directive précise que celle-ci « n'affecte pas la protection des personnes physiques à l'égard du traitement des données à caractère personnel garanti par le droit de l'Union et le droit des États membres, en particulier le [RGPD] [...], mais aussi et y compris de toute disposition de droit national complémentaire. »

Il convient dès lors de trouver un juste équilibre entre le droit fondamental de l'accès à l'information¹ et le droit fondamental à la protection des données à caractère personnel, dans la limite des règles applicables en matière de droit d'accès prévu par la législation nationale.

Cet équilibre doit être recherché quand un document contenant des données à caractère personnel est susceptible d'être communiqué.

Les règles d'accès aux documents contenant des données à caractère personnel

À titre liminaire, il convient de préciser que, comme le relèvent les auteurs dans l'exposé des motifs accompagnant le projet de loi, un « document qui n'est pas accessible, ne peut pas être mis à disposition du public par le biais de l'Open data ».

L'article 1^{er}, paragraphe (3) du projet de loi indique que la « loi s'appuie sur les règles d'accès en vigueur et ne les affecte en rien ». Suivant le commentaire des articles, « si pour

¹ Ce droit fondamental découle notamment du droit à la liberté d'expression, du droit à une bonne administration et du droit d'accès aux documents.

des motifs de protection des données les règles d'accès excluent l'accès aux documents, ces documents ne relèvent pas du champ d'application du présent projet de loi ». D'après les auteurs du projet de loi, les règles d'accès générales découlent de la loi modifiée du 14 septembre 2018 relative à une administration transparente et ouverte et sont complétées par des règles d'accès sectorielles ou spécifiques, découlant notamment

- de la loi modifiée du 25 novembre 2005 concernant l'accès du public à l'information en matière d'environnement ;
- de la loi modifiée du 31 juillet 2005 portant approbation de la Convention sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement, faite à Aarhus (Danemark), le 25 juin 1998 ;
- du règlement grand-ducal du 8 juin 1979 relatif à la procédure à suivre par les administrations relevant de l'Etat et des communes.

L'article 1^{er}, paragraphe (1), du projet de loi vise les « *documents existants détenus par des organismes du secteur public* » ainsi qu'une liste d'« *entreprises publiques* » et des « *données de la recherche* », sous réserve des exceptions et conditions définies aux paragraphes (2) à (7). Or, la loi précitée du 14 septembre 2018 vise, en son article 1^{er}, paragraphe 1, l'accès aux « *documents détenus par les administrations et services de l'État, les communes, les syndicats de communes, les établissements publics placés sous la tutelle de l'État ou sous la surveillance des communes ainsi que les personnes*

morales fournissant des services publics ». La CNPD se demande si les champs d'application respectifs du projet de loi et de la loi du 14 septembre 2018 couvrent les mêmes entités.

Par conséquent, la CNPD s'interroge quant à l'existence de règles d'accès applicables aux documents détenus par des entreprises publiques qui ne sont pas relatifs à l'exercice d'une activité administrative. En l'absence de telles règles d'accès, la diffusion de documents contenant des données à caractère personnel devrait en principe être exclue, à moins que le responsable de traitement ne puisse démontrer qu'une telle opération de traitement de données, c'est-à-dire la transmission des données à caractère personnel à un tiers, puisse être justifiée à l'égard des dispositions pertinentes en matière de protection des données. Il pourrait par exemple être envisageable de récolter le consentement des personnes concernées.

Toutefois, la CNPD rappelle le considérant 154 du RGPD qui prévoit que « [...] [*Les données à caractère personnel figurant dans des documents détenus par une autorité publique ou un organisme public devraient pouvoir être rendues publiques par ladite autorité ou ledit organisme si cette communication est prévue par le droit de l'Union ou le droit de l'État membre dont relève l'autorité publique ou l'organisme public. [...]* ». Ainsi, en principe, la communication de tels documents devrait être prévue par une disposition légale.

La Commission nationale comprend que l'article 1^{er}, paragraphe (2), point 8^o du projet

6

ANNEXES

de loi reflète fidèlement l'article premier, paragraphe (2), lettre h) de la directive. Ladite disposition de la directive reprend les termes du considérant 154, *in fine*, du RGPD. La CNPD conçoit également que la marge de manœuvre du législateur est limitée en matière de transposition fidèle d'une directive européenne. Néanmoins, les directives européennes visent l'harmonisation des règles nationales sans pour autant exiger une uniformité de celles-ci et permettent ainsi au législateur d'adapter les normes de transpositions aux spécificités nationales. La CNPD attire l'attention sur la portée de ladite disposition du projet de loi, qui prévoit que la

« [...] loi ne s'applique pas [...] aux documents dont l'accès est exclu ou limité en application de règles d'accès pour des motifs de protection des données à caractère personnel, et aux parties de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été définie par la loi comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel ou comme portant atteinte à la protection de la vie privée et de l'intégrité de la personne concernée ».

Il n'est pas à exclure que des règles d'accès sectorielles, telles que celles identifiées plus haut, puissent prévoir l'accès à des documents contenant des données à caractère personnel, alors que les règles d'accès générales découlant de la loi précitée du 14 septembre 2018 limitent la

communication des documents contenant des données à caractère personnel.

De plus, en l'absence d'une disposition légale spécifique au sens de l'article 1^{er} paragraphe (2), point 8^o du projet de loi applicable aux données à caractère personnel contenues dans le document rendu accessible en vertu des règles d'accès, ce document peut relever du champ d'application du projet de loi.

Dès lors, lorsque la législation sectorielle applicable au document reste muette, c'est-à-dire qu'elle n'exclut pas explicitement la réutilisation des données à caractère personnel, la CNPD s'inquiète du risque de divulgation de données à caractère personnel ou de l'atteinte à la vie privée des personnes physiques.

La CNPD rappelle le considérant 154 du RGPD précité que « [c]es dispositions légales devraient concilier l'accès du public aux documents officiels et la réutilisation des informations du secteur public, d'une part, et le droit à la protection des données à caractère personnel, d'autre part, et peuvent dès lors prévoir la conciliation nécessaire avec le droit à la protection des données à caractère personnel en vertu du [RGPD] ». Il revient ainsi au législateur de soupeser l'intérêt public lié à l'accès et la réutilisation des données en relation avec les intérêts des personnes physiques.

D'une part, la Commission nationale recommande dès lors au législateur de revoir les règles d'accès, en particulier les règles d'accès sectorielles, afin de s'assurer que celles-ci excluent,

lorsque cela est pertinent, l'accès aux documents contenant des données à caractère personnel ou que celles-ci prévoient *a minima* l'anonymisation des données à caractère personnel.

D'autre part, la CNPD estime nécessaire d'analyser les traitements de données à caractère personnel susceptibles d'être visées par des règles d'accès et invite le législateur, le cas échéant, de modifier les législations sectorielles y afférentes, notamment dans le secteur de l'environnement et des données issues du monde agricole afin d'y insérer, si nécessaire, une limitation quant à l'accès aux ou la publication de données à caractère personnel.

Finalement, lorsque des données à caractère personnel sont néanmoins susceptibles d'être rendues publiques sur la base des règles d'accès et en l'absence de dispositions législatives empêchant leur réutilisation, il pourrait s'avérer nécessaire pour un responsable de traitement, c'est-à-dire de l'organisme mettant à disposition le document, de faire une analyse d'impact relative à la protection des données au sens de l'article 35 du RGPD avant de mettre un document à disposition dans laquelle la mise en balance de l'intérêt public et des intérêts des personnes concernées est opérée. Ainsi, lorsque l'évaluation des risques pour les droits et libertés des personnes concernées révèle que la communication du document représente un risque élevé, l'organisme devrait s'abstenir à mettre à disposition le document, à moins que des mesures pour atténuer le risque, notamment par l'anonymisation du document publié, puissent être pris.

Les règles applicables à la divulgation et à la réutilisation de données à caractère personnel

Puisque le présent projet de loi n'affecte en rien les règles d'accès en vigueur, la CNPD rappelle qu'il est tout à fait envisageable qu'un document soit accessible en vertu de ces règles d'accès mais qu'il ne soit pas pour autant réutilisable au sens du texte sous considération, eu égard notamment aux règles de la protection des données à caractère personnel.

En effet, l'article 1^{er}, paragraphe (4), point 10^o du projet de loi prévoit que la « *présente loi est sans préjudice des dispositions de droit sur la protection des données à caractère personnel* ». Il ressort de cette disposition que, lorsque la réutilisation d'un document contenant des données à caractère personnel est possible, les responsables de traitement – c'est-à-dire l'entité mettant le document à disposition et l'entité souhaitant réutiliser ledit document – continuent d'être liés par les dispositions applicables en matière de protection des données, en premier lieu par les dispositions découlant du RGPD et de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Dans l'exposé des motifs accompagnant le projet de loi, les auteurs font état d'une future stratégie nationale pour la promotion de l'Open data au Luxembourg qui sera définie autour, entre autres éléments, du concept de l'« *ouverture dès la conception et par défaut* ».

6

ANNEXES

Cela signifie que les détenteurs de données publiques devraient concevoir lesdites données dans l'optique de rendre celles-ci réutilisables. La présence de données à caractère personnel dans un jeu de données peut entraver sa publication par l'organisme et sa réutilisation par un tiers.

En matière de protection des données, en vertu de l'article 25 du RGPD, les responsables de traitement doivent appliquer la protection des données dès la conception et protection des données par défaut, notamment à travers du respect du principe de minimisation des données, c'est-à-dire 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 » tel que prévu à l'article 5, paragraphe (1), lettre c), du RGPD.

Par conséquent, l'organisme ou l'entreprise publique devraient préparer les documents dès leur création avec un minimum de données à caractère personnel, en perspective d'une part du respect des principes de la protection des données et d'autre part de l'objectif de la réutilisation des informations. Ainsi, un plus grand nombre de documents pourraient potentiellement se retrouver dans le champ d'application du présent projet de loi.

À cet égard, malgré le fait que l'anonymisation de données à caractère personnel soit définie à l'article 2, point 7° du projet de loi et que les coûts d'une éventuelle anonymisation peuvent entrer en ligne de compte pour la tarification

conformément à l'article 7 du projet de loi et du projet de règlement grand-ducal, la Commission nationale regrette que le projet de loi ne prévoit pas que ce procédé soit appliqué de manière générale aux documents entrant dans le champ d'application du projet de loi.

La définition de l'anonymisation à l'article 2, point 7° du projet de loi devra être lue ensemble avec les dispositions du RGPD, et notamment avec le considérant 26 du RGPD :

« Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. [...] »

Le Comité Européen de la Protection des Données (EDPB) a considéré, dans ses lignes directrices 4/2019 relatives à l'article 25 du RGPD sur la protection des données dès la conception et protection des données par défaut, que l'anonymisation de données à caractère personnel est une alternative à la suppression pour autant que les éléments

contextuels pertinents aient été pris en compte et que la probabilité ainsi que la gravité du risque, y compris le risque de ré-identification, soient régulièrement réévaluées².

Le groupe de travail « Article 29 », dans son avis n° 5/2014 sur les techniques d'anonymisation, explique que

« l'anonymisation est le résultat du traitement des données personnelles afin d'empêcher, de façon irréversible, toute identification. Ce faisant, les responsables du traitement des données doivent tenir compte de plusieurs éléments, en prenant en considération l'ensemble des moyens 'susceptibles d'être raisonnablement mis en œuvre' à des fins d'identification (soit par le responsable du traitement, soit par un tiers) »³.

Ainsi, la CNPD souligne qu'il est important que le choix des techniques d'anonymisation se fasse sur la base d'une analyse au cas par cas prenant en compte le contexte des données, tout en veillant à rendre les données effectivement anonymes et ainsi échapper à l'application du RGPD.

Lorsque l'anonymisation est faite dans les règles de l'art, suivant le considérant 26 du RGPD

« [...] Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de

telle manière que la personne concernée ne soit pas ou plus identifiable. Le [RGPD] ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche. »

Par conséquent, à l'issue du processus d'anonymisation, il ne s'agit plus de donnée à caractère personnel et le RGPD ainsi que les autres règles en matière de protection des données à caractère personnel ne sont plus applicables.

Lorsque les données à caractère personnel semblent néanmoins indispensables à la compréhension du document, en vertu du principe de minimisation des données, il convient de les limiter à ce qui est nécessaire.

Le considérant 52 de la directive précise notamment « *que la réutilisation de données à caractère personnel n'est licite que si le principe de limitation des finalités énoncé à l'article 5, paragraphe 1, point b), et à l'article 6 du [RGPD] est respecté.* ».

En vertu de l'article 9, alinéa 1^{er}, du projet de loi, la « *réutilisation de documents peut être soumise à [des] conditions pour autant que celles-ci soient objectives, proportionnées, non discriminatoires et justifiées sur la base d'un objectif d'intérêt général* ». La Commission nationale estime que le recours à des licences, dans la mesure où elles porteraient également sur les conditions de réutilisation des données à caractère personnel contenues dans un document, pourrait permettre de réduire

² EDPB, lignes directrices 4/2019 relatives à l'article 25 du RGPD sur la protection des données dès la conception et protection des données par défaut, version du 13 novembre 2019 soumise à la consultation publique, non encore adoptée définitivement.

³ Groupe de travail « Article 29 » sur la protection des données, Avis n°05/2014 sur les techniques d'anonymisation, WP216, 0829/14/FR.

6

ANNEXES

indirectement les risques pour les personnes concernées en imposant des garanties supplémentaires à prévoir par l'entité souhaitant réutiliser le document.

Toutefois, la Commission nationale appelle à la prudence quant à la mise à disposition de données à caractère personnel au vu du risque de réutilisation à des fins non compatibles par des tiers en ce que la Commission nationale note que l'entité publique n'a qu'une influence limitée sur cette réutilisation.

Indépendamment de ces considérations, le responsable de traitement qui souhaiterait réutiliser les documents contenant des données à caractère personnel devrait lui aussi vérifier si le traitement de données à caractère personnel contenues dans le document peut se faire en conformité avec les obligations en matière de protection des données en vérifiant en particulier la nécessité et la proportionnalité du traitement de données envisagé en lien avec la finalité poursuivie.

Le règlement grand-ducal n'appelle quant à lui pas d'observations particulières de la part de la CNPD.

Ainsi décidé à Belvaux en date du 20 janvier 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

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 1^{er} 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 8 juillet 2019, la CNPD a avisé le projet de loi n°7425 portant : 1^o transposition de la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes ; 2^o modification du Code pénal, et 3^o abrogation de la loi du 20 avril 1881 concernant le transport et le commerce des matières explosives (ci-après le « projet de loi »).

La Commission de la Justice a adopté lors de sa réunion du 27 mai 2020 une série d'amendements relative au projet de loi.

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°7425 portant : 1^o transposition de la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes ; 2^o modification du Code pénal, et 3^o abrogation de la loi du 20 avril 1881 concernant le transport et le commerce des matières explosives. (Délibération n°2/2021 du 4/02/2021)

Dans la mesure où certains de ces amendements concernent des articles qui ont été commentés par la Commission nationale dans son avis du 8 juillet 2019, la CNPD s'autosaisit pour les aviser.

A titre de remarque liminaire, elle se félicite que les auteurs du projet de loi aient uniformisé la terminologie employée en ce qui concerne la désignation du fichier tenu par le Ministre ayant dans ses compétences la loi sous avis (ci-après le « ministre ») conformément à l'article 15 (13 initial) du projet de loi, tel que cela avait été suggéré par la Commission nationale.

Toutefois, elle aimerait revenir plus en détail sur la vérification d'honorabilité (I), sur le fichier des armes (II), sur l'attestation médicale (III), sur le registre des armes (IV), et sur l'autorité de contrôle compétente en cas d'accès par les agents de l'Administration des douanes et accises au fichier des armes (V).

1. Sur la vérification d'honorabilité

L'amendement n°14 insère un article 14 nouveau intitulé « Vérification d'honorabilité », en vertu duquel le ministre diligentera l'enquête

6

ANNEXES

administrative et sera, dans le cadre de cette mission, amené à traiter des données à caractère personnel initialement collectées et traitées par la Police grand-ducale, par le Ministère public ou par le Service de renseignement de l'Etat (ci-après le « SRE ») 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. Ces traitements initiaux sont soumis 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 convient de relever que les traitements de données à caractère personnel mis en œuvre dans le cadre de l'enquête administrative, telle que visée à l'article 14 nouveau du projet de loi sous avis, seront soumis au RGPD alors que la finalité poursuivie par le ministre est la délivrance d'une autorisation, d'un permis ou agrément prévus par le projet de loi sous avis. Les finalités poursuivies par le ministre seraient donc étrangères aux finalités initiales énoncées ci-avant.

Ainsi, bien que les finalités du traitement, envisagé par l'article 14 du projet de loi, soient à des fins administratives, la nature même des données transmises au ministre et ensuite utilisées pour diligenter l'enquête administrative reste identiques à la nature des données traitées 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. Dans un tel contexte,

il y a lieu de s'interroger sur l'articulation des dispositions du RGPD avec celles de la loi du 1^{er} 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.

1. Sur le traitement effectué par le ministre dans le cadre de l'enquête administrative

A. Sur le principe de la licéité du traitement

La CNPD salue le fait que l'article 14 nouveau du projet de loi sous avis, d'un point de vue de la sécurité juridique, constitue la base légale de l'enquête administrative effectuée par le ministre, conformément à l'article 6 paragraphe (3) du RGPD.

a. Sur l'article 6 paragraphe (3) du RGPD

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)⁴ qui dispose que « *[l]e 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.*

⁴ 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; (...)* ».

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.»

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'Etat 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 Etat 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 énonce encore que « [l]orsque 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'Etat 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. ».

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

6

ANNEXES

finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

Toutefois et bien que la base légale instaurant l'enquête administrative précise les types de données traitées, les personnes concernées ainsi que les entités auxquelles les données peuvent être communiquées et pour quelles finalités, la Commission nationale relève que certains éléments relatifs au traitement de données ne sont pas suffisamment précisés ou ne sont pas précisés du tout (par exemple la durée de conservation des données) dans le projet de loi.

b. Sur les principes dégagés par la jurisprudence de la Cour européenne des droits de l'Homme et de la Cour de justice de l'Union européenne

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.

i. Sur 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 « *prévues par la loi* », au sens de l'article 8 paragraphe (2) de la Convention européenne des droits de l'homme⁵, que si elle repose sur un article du droit national qui présente certaines caractéristiques. L'expression « *prévues 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 Convention⁶. La législation interne doit être « *accessible aux personnes concernées et prévisible quant à*

⁵ 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* ».

⁶ CouEDH, *Fernández Martínez c. Espagne* [GC], n°56030/07, para. 117.

ses répercussions »⁷. 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 »⁸ ainsi que « [l]e degré de précision requis de la "loi" à cet égard dépendra du sujet en question. »⁹.

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. Cet encadrement légal serait par ailleurs un garant du principe de sécurité juridique au profit des personnes concernées, les demandeurs d'une autorisation, permis ou agrément prévus par le projet de loi sous avis. 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 conséquence¹⁰.

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 »¹¹. 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 »¹². 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 »¹³.

Dès lors, dans la mesure où les traitements de données mis en œuvre par le ministre dans le

⁷ 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.

⁸ 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.

⁹ CouEDH, *The Sunday Times c. Royaume-Uni*, n° 6538/74, 26 avril 1979, para. 49 ; voir également 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.

¹⁰ Voir p.ex. Cour EDH, *Aurubis Balgaría* du 31 mars 2011, C-546/09, points 42-43 ; Arrêt, *Alfamicro c. Commission* du 14 novembre 2017, T-831/14, points 155-157.

¹¹ Cour EDH, *Amann c. Suisse* [GC], n° 27798/95 para 56.

¹² *Ibidem*. Voir également Cour EDH, *Malone c. Royaume-Uni*, série An°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*, no 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.

¹³ Arrêt du 8 avril 2014, *Digital Rights Ireland e.a. C-293/12 et C-594/12*, EU :C:2014 :238, point 54.

6

ANNEXES

cadre de l'enquête administrative constituent une ingérence dans le droit au respect de la vie privée des demandeurs d'une autorisation, d'un permis ou agrément, le projet de loi devrait encadrer plus spécifiquement de tels traitements conformément à la jurisprudence de la Cour européenne des droits de l'Homme. Or, force est de constater que le projet de loi sous avis, tel qu'amendé n'est, par endroit, pas rédigé avec suffisamment de précision¹⁴. Elle reviendra sur ce point dans les développements aux points D, E et F ci-après.

ii. Sur la seconde condition

Il ressort de la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'Homme que les motifs invoqués par les autorités publiques pour justifier une limitation à l'exercice du droit à la protection des données à caractère personnel ou une ingérence dans le droit au respect de la vie privée doivent être pertinents et suffisants¹⁵ et qu'il doit être démontré qu'il n'existe pas d'autres méthodes moins intrusives¹⁶. La notion de nécessité, telle qu'interprétée par la Cour de justice de l'Union européenne, implique que les mesures adoptées soient moins intrusives que d'autres options pour atteindre le même but. De plus, selon la jurisprudence de la Cour européenne des droits de l'Homme, pour répondre au critère de nécessité, l'ingérence devra également être proportionnée. Dans son « Manuel de droit européen en matière de protection des données », l'Agence des droits fon-

damentaux de l'Union européenne précise que « [l]a proportionnalité requiert qu'une mesure d'ingérence dans l'exercice des droits protégés par la Cour européenne des droits de l'Homme n'aille pas au-delà de ce qui est nécessaire pour atteindre le but légitime poursuivi. Les facteurs importants à prendre en compte lors de l'appréciation du critère de proportionnalité sont la portée de l'ingérence, notamment le nombre de personnes concernées, et les garanties ou les avertissements mis en place pour limiter sa portée ou ses effets négatifs sur les droits des individus »¹⁷.

Le Contrôleur européen de la protection des données indique encore qu'« [u]n examen de la proportionnalité suppose en règle générale de déterminer quelles « garanties » doivent accompagner une mesure (qui porterait par exemple sur la surveillance) afin de réduire à un niveau « acceptable »/proportionné les risques posés par la mesure envisagée au regard des droits fondamentaux et des libertés des individus concernés. »¹⁸.

En l'occurrence, la Commission nationale se demande à défaut de telles précisions, quelles seraient les garanties envisagées par les auteurs du projet de loi sous avis et s'il n'existerait pas de méthodes moins intrusives que le système prévu par le dispositif sous avis.

Il ressort du texte sous avis que le déroulement de l'enquête administrative engendrera une duplication des informations concernant les

¹⁴ 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

¹⁵ Voir l'arrêt de la Cour européenne des droits de l'homme du 4 décembre 2008, S. et Marper c. Royaume-Uni.

¹⁶ Voir les arrêts de la Cour de justice du 9 novembre 2010, C-92/09, Volker und Markus Schecke GbR/Land Hessen, et C-93/09, Eifert/Land Hessen et Bundesanstalt für Landwirtschaft und Ernährung.

¹⁷ Voir page 45 du « Manuel de droit européen en matière de protection des données » de l'Agence des droits fondamentaux de l'Union européenne.

¹⁸ Voir page 11 des « Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel ».

antécédents judiciaires d'une personne dans les mains de différentes autorités. En effet, la Commission nationale comprend que certaines des données contenues dans les fichiers tenus par la Police grand-ducale, par le Ministère public ou le SRE seront amenées à figurer une nouvelle fois dans un fichier tenu par le ministre.

Afin d'éviter une duplication de telles données et la tenue d'une sorte de nouveau « *casier bis* » par le ministre pour les personnes concernées par la loi en projet, la CNPD estime qu'une méthode moins intrusive pour atteindre le même but devrait être préférée au système actuellement prévu par les auteurs du projet de loi. Elle se rallie, ainsi, à la proposition faite par le Conseil d'Etat dans son avis complémentaire du 19 décembre 2020¹⁹ selon lequel il propose le mécanisme d'un avis circonstancié émis par le procureur d'Etat et transmis au ministre. Ce mécanisme se substituerait à la communication au ministre de renseignements par la Police grand-ducale, le Ministère public et le SRE.

Un tel mécanisme permettrait d'éviter une duplication des données concernant les antécédents judiciaires d'un demandeur tout en permettant au ministre d'obtenir les informations nécessaires et pertinentes,

sous forme d'un avis, afin de lui permettre d'apprécier l'« *honorabilité* » d'un demandeur. Un tel mécanisme présente encore l'avantage que l'enquête administrative serait confiée à une autorité répressive, le Ministère public, et non pas à une administration. En effet, une telle autorité serait plus appropriée pour mener une telle enquête eu égard à la nature des données traitées.

iii. Sur le système belge et français

Il est intéressant de noter qu'une approche similaire a été adoptée en Belgique et en France.

En effet, en Belgique, le gouverneur, qui est l'autorité compétente pour délivrer des agréments ou autorisation pour la détention d'une arme à feu, statue sur la demande après avoir reçu l'avis motivé du procureur du Roi et du bourgmestre compétents²⁰ ou après avis du chef de corps de la police locale²¹.

En France, le préfet qui est l'autorité compétente pour délivrer les autorisations en matière d'armes²², se verra lui aussi communiquer l'« *avis du service national des enquêtes administratives de sécurité* » et l'« *avis issu de l'enquête administrative diligentée par les services de police ou de gendarmerie* » afin de délivrer lesdites autorisations.

¹⁹ Avis complémentaire du Conseil d'Etat du 19 décembre 2020, document parlementaire n°7425/08, développements sous « Amendement 14 ».

²⁰ En ce qui concerne les agréments d'armuriers, intermédiaires, collectionneurs d'armes et de toute personne exerçant certaines activités professionnelles impliquant la détention d'armes à feu, l'article 11 paragraphe (1) de la loi du 8 juin 2006 précitée dispose que : « [c]ette autorisation ne peut être délivrée qu'après avis, dans les trois mois de la demande, du chef de corps de la police locale de la résidence du requérant. La décision doit être motivée. (...) S'il apparaît que la détention de l'arme peut porter atteinte à l'ordre public ou que le motif légitime invoqué pour obtenir l'autorisation n'existe plus, le gouverneur compétent pour la résidence de l'intéressé peut limiter, suspendre ou retirer l'autorisation par décision motivée selon une procédure définie par le Roi et après avoir pris l'avis du procureur du Roi compétent pour cette résidence. ».

²¹ En ce qui concerne la délivrance d'une autorisation pour la détention d'une arme à feu par un particulier, l'article 11 paragraphe (1) de la loi du 8 juin 2006 précitée dispose que : « [c]ette autorisation ne peut être délivrée qu'après avis, dans les trois mois de la demande, du chef de corps de la police locale de la résidence du requérant. La décision doit être motivée. (...) S'il apparaît que la détention de l'arme peut porter atteinte à l'ordre public ou que le motif légitime invoqué pour obtenir l'autorisation n'existe plus, le gouverneur compétent pour la résidence de l'intéressé peut limiter, suspendre ou retirer l'autorisation par décision motivée selon une procédure définie par le Roi et après avoir pris l'avis du procureur du Roi compétent pour cette résidence. ».

²² Article R.312-2 du Code de la sécurité intérieure française.

6

ANNEXES

Par conséquent, afin de répondre au critère de nécessité, la CNPD recommande aux auteurs du projet de loi de s'inspirer du système mis en place par les législations belges et françaises et de suivre les suggestions émises par le Conseil d'Etat, comme mentionné ci-avant.

Enfin, sous réserve que les auteurs du projet de loi maintiennent le système envisagé par le projet de loi sous avis, la Commission nationale entend faire les commentaires ci-après.

B. Sur l'origine des données traitées par le ministre

La Commission nationale comprend que les données collectées et traitées par le ministre dans le cadre de l'enquête administrative proviennent de fichiers tenus par la Police grand-ducale, le Ministère public et le SRE. Ces données ont été initialement collectées par les autorités précitées 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. L'article 14 nouveau prévoit que ces autorités communiquent au ministre de telles données dans le cadre de l'enquête administrative.

La CNPD se félicite qu'une telle base légale soit prévue par le dispositif sous avis conformément aux dispositions de l'article 8 paragraphe (1) de la loi du 1^{er} 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.

Cet article dispose que « *[l]es données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées à l'article 1^{er} ne peuvent être traitées à des fins autres que celles y énoncées, à moins qu'un tel traitement ne soit autorisé par le droit de l'Union européenne ou par une disposition du droit luxembourgeois.* ».

Par ailleurs, il y a lieu de relever que cette base légale semble instaurer un régime spécial par rapport aux dispositions de la section 2, chapitre 2, de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière, et à celles prévues par l'article 9 paragraphe (2) de la loi modifiée du 5 juillet 2016 portant réorganisation du SRE.

En effet, ces dispositions ont respectivement pour objet d'encadrer la transmission de telles données par la Police grand-ducale à d'autres administrations dans le cadre de la vérification de l'honorabilité²³, et la communication par le SRE « *[d]es renseignements collectés dans le cadre de ses missions (...) aux administrations dans la mesure où ces renseignements paraissent utiles à l'accomplissement de leurs missions respectives.* »²⁴.

En tout état de cause, il convient de saluer le fait que cette base légale prévoit expressément la communication des données visées à l'article 14 nouveau par le Ministère public au ministre dans le cadre de l'enquête administrative alors qu'à ce jour aucune disposition légale ne prévoyait une telle communication. Ce d'autant plus, eu

²³ Voir document parlementaire n°6975 sur le projet de loi relative à l'échange de données à caractère personnel et d'informations en matière policière, commentaires des auteurs du projet de loi concernant les articles 26 et suivants du projet de loi.

²⁴ Article 9 paragraphe (2) de la loi modifiée du 5 juillet 2016 portant réorganisation du SRE.

égard à la récente affaire dite du « casier bis » ou « Jucha ».

Enfin, et afin de permettre aux personnes concernées de comprendre l'étendue et la portée de l'enquête administrative, ne serait-il pas préférable d'indiquer expressément à l'article 14 nouveau que les données collectées lors de l'enquête administrative proviennent des fichiers tenus par la Police grand-ducale, le Ministère public ou le SRE ?

Quant aux fichiers tenus par la Police grand-ducale, il y a lieu d'attirer l'attention des auteurs du projet de loi sur le projet de loi n°7741 portant modification 1° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, 2° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat et 3° du Code pénal, déposé le 30 décembre 2020 (ci-après le « projet de loi n°7741 »). Le projet de loi n°7741 a pour objet d'encadrer les traitements des données à caractère personnel effectués dans les fichiers de la Police grand-ducale, et plus précisément dans le fichier central.

L'article 43-2 du projet de loi n°7741 prévoit que le fichier central disposera d'une partie passive (quant aux informations qui seraient transmises dans la partie passive du fichier central, il est renvoyé au projet de loi n°7741). Il y a lieu de relever que l'accès à la partie passive du fichier central sera strictement limité aux finalités énumérées au paragraphe (19) de l'article 43-2 du projet de loi n°7741. Cette consultation ne sera, en outre, possible qu'avec l'accord du procureur

général d'Etat. Dès lors et dans la mesure où la consultation à des fins de réalisation d'une enquête administrative, telle que prévue par l'article 14 nouveau du projet de loi, ne semble pas être visée par l'article 43-2 précité, il y a lieu de s'interroger sur l'articulation des dispositions prévues par le projet de loi n°7741 avec celles du projet de loi sous avis.

C. Sur le principe de limitation des finalités

Conformément au principe de 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.

Il y a lieu de relever que la transmission des données provenant de fichiers tenus par la Police grand-ducale, le Ministère public ou encore le SRE vers le ministre, à des fins d'enquête administrative, est très délicate voire risquée et doit, dès lors, être limitée à des situations exceptionnelles et strictement limitées.

Ainsi, l'utilisation des données à des fins autres que celles pour lesquelles ont été transmises au ministre, comporte des risques additionnels et semble a priori difficilement justifiable. Une telle utilisation ultérieure devrait en tout état de cause respecter les conditions de l'article 6 paragraphe (4) du RGPD et faire l'objet d'une loi « *du moins quant aux éléments essentiels de la matière* » conformément à l'article 11, paragraphe (3) de la Constitution²⁵.

²⁵ Voir en ce sens, M. Besch, « Traitement de données à caractère personnel dans le secteur public », Normes et légistique en droit public luxembourgeois, Luxembourg, Promoculture Larcier, 2019, p.471 à 472, n°619.

6

ANNEXES

Par conséquent, à l'instar des dispositions prévues à l'article 26 paragraphes (2) et (3) de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière²⁶, ne faudrait-il pas prévoir dans le projet de loi sous avis que les données transmises au ministre, à des fins d'enquête administrative, ne peuvent être utilisées que pour la finalité pour laquelle elles ont été transmises et encadrer la transmission, le cas échéant, par le ministre à une autre administration/ à un tiers ?

Par ailleurs, il est intéressant de noter que la loi allemande du 17 février 2020 sur les armes prévoit que les données collectées dans le contexte de la vérification de l'honorabilité ne peuvent être utilisées qu'à cette fin dans le cadre de la loi sur les armes. Le § 5 « Zuverlässigkeit », (5) précise que « (...) Die nach Satz 1 Nummer 2 erhobenen personenbezogenen Daten dürfen nur für den Zweck der waffenrechtlichen Zuverlässigkeitsprüfung verwendet werden ».

D. Sur le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes

L'article 10 du RGPD dispose que « [l]e traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État

membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. ». Ledit article précise encore que « [t]out registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique ».

Force est de constater que pareilles garanties ne semblent pas avoir été prévues par les auteurs du projet de loi, ou alors celles-ci ne sont pas précisées par ces derniers dans le dispositif sous avis ni dans leur commentaire de l'article 14 nouveau.

Or, il est essentiel que de telles garanties soient prévues dans le projet de loi alors qu'en l'état actuel du dispositif sous avis, les personnes concernées verront une duplication de leurs données relatives à des condamnations pénales ou à des infractions aux mains de plusieurs autorités. La collecte de telles données lors de l'enquête administrative pourrait aboutir à la tenue d'une sorte de nouveau « casier bis » par le ministre. Celui-ci disposerait, le cas échéant, à l'issue de l'enquête de la copie de rapports de police, extraits de procès-verbaux, jugements, ou encore des « *informations nécessaires* » fournies par le SRE.

En outre, il y a encore lieu de s'interroger sur la question de l'exactitude et de la mise à jour des données qui seraient transmises par le Ministère public, la Police grand-ducale ou par le SRE au ministre alors que le système envisagé ne prévoit pas un retour de ces autorités vers le ministre. Par exemple, cette question pourrait se poser dans l'hypothèse

²⁶ L'article 26 paragraphes (2) et (3) dispose que : « (2) Les données et informations transmises ne peuvent être utilisées par l'administration que pour la finalité pour laquelle elles ont été transmises. Elles sont effacées dès que leur conservation n'est plus nécessaire au regard de la finalité pour laquelle elles ont été transmises. (3) La transmission ultérieure des données et informations par l'administration de l'État à une tierce personne requiert l'accord préalable écrit de la personne visée à l'article 18, paragraphe 1 er, ayant transmis les données et informations concernées. Le cas échéant, l'article 6, paragraphe 3, est applicable ».

où des données transmises par la Police grand-ducale ou le SRE, et relatives à des faits concernant un requérant aboutiraient à une décision de non-lieu, un classement sans suite.

La CNPD estime donc essentiel que des garanties soient prévues par les auteurs du projet de loi. La transmission d'un avis circonstancié du Ministère public à la place des transmissions actuellement prévues par le projet de loi, tel que suggéré par le Conseil d'Etat, pourrait être l'une d'entre elles.

E. Sur le traitement de catégories particulières de données à caractère personnel

A titre de remarque liminaire, il y a lieu de souligner que si les données transmises par le SRE au ministre le sont pour des finalités administratives, il n'en reste pas moins que la nature même des données ne changera pas. Dans ce contexte, il y a lieu de s'interroger sur l'applicabilité de la loi du 1^{er} 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.

Dans le cadre de l'échange de données entre le SRE et le ministre, tel que prévu au paragraphe (6) de l'article 14 nouveau du projet de loi sous avis, la CNPD comprend que, dans ce contexte, des catégories particulières de données, au sens de l'article 9 du RGPD, seraient susceptibles d'être communiquées au ministre.

En effet, les auteurs du projet loi précisent que ce paragraphe a été introduit compte tenu du « *contexte politique actuel au niveau des tendances extrémistes violentes* », contexte qui « *démontre l'importance pour les autorités de pouvoir vérifier plus en détail la personne qui soumet une autorisation d'acquérir, d'acheter, d'importer, d'exporter, de transférer, de transporter, de détenir, de porter, de vendre et de céder des armes et munitions* ».

Dès lors, il y a lieu de s'interroger sur le fait de savoir si des données relatives aux opinions politiques voir aux convictions religieuses ou philosophiques d'une personne sollicitant un agrément, permis ou autorisation seraient susceptibles d'être communiquées au ministre. Dans l'affirmative, il s'agirait d'un traitement de catégories particulières de données.

A ce titre, il est rappelé que le traitement de catégories particulières de données est, en principe, interdit par l'article 9 paragraphe (1) du RGPD²⁷ sauf si une des conditions visées au paragraphe (2) dudit article s'applique.

La Commission nationale estime que le traitement de catégories particulières de données, lors de l'enquête administrative par le ministre, pourrait se baser sur l'article 9 paragraphe (2) du RGPD. Cet article dispose que « *[l]e 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*

²⁷ L'article 9 paragraphe (1) dispose que : « *[l]e traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits* ».

6

ANNEXES

et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée».

A défaut de précision des « *mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* », le projet de loi sous avis ne semble pas offrir un fondement juridique suffisant pour traiter ces catégories de données particulières.

Afin de rendre licite un tel traitement de données par le ministre, la Commission nationale estime indispensable que de telles mesures soient définies dans le projet de loi sous avis.

Il conviendrait également de préciser expressément que des catégories particulières de données pourraient être collectées alors que cela ne résulte pas de la lecture du paragraphe (6) de l'article 14 nouveau du projet de loi. Ainsi, il est suggéré que les auteurs du projet de loi s'inspirent des dispositions françaises visées à l'article R.312-85 point VI du Code de la sécurité intérieure intitulé « données et informations issues de l'enquête administrative ».

Cet article dispose que « *[p]ar dérogation, sont autorisés, en cas de nécessité absolue pour les seules fins et dans le respect des conditions applicables à ce traitement, la collecte, la conservation et le traitement de données strictement nécessaires, adéquates et non excessives qui figurent dans l'enquête administrative mentionnée au V et relatives :*

1° Aux opinions politiques, aux convictions

religieuses, à l'appartenance syndicale ou à la santé de la personne faisant l'objet de cette enquête administrative ;

2° A la prétendue origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses, à l'appartenance syndicale, à la vie sexuelle ou l'orientation sexuelle d'une personne autre que celle faisant l'objet de l'enquête administrative mentionnée au V, sous réserve que ces données se rapportent à une procédure dans laquelle la personne faisant l'objet de l'enquête administrative est mise en cause. ».

F. Sur le principe de minimisation des données

Outre le fait que les dispositions des articles 10 et 9 du RGPD devront être respectées, le principe de minimisation devra également être respecté lors de la mise en œuvre du traitement visé à l'article 14 nouveau.

Conformément à ce principe, 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. La minimisation des données signifie que le responsable du traitement doit uniquement traiter les données qui sont nécessaires (et non seulement utiles) à la réalisation des finalités.

S'il y a lieu de féliciter les auteurs du projet de loi pour avoir délimité les faits sur lesquels l'enquête administrative portera, des précisions quant aux données qui seront effectivement communiquées au ministre, lors de l'enquête

administrative, mériteraient d'être apportées.

En l'absence de telles précisions, la Commission nationale n'est pas en mesure d'apprécier si le principe de minimisation des données serait respecté et tient à soulever les points ci-après.

a. Sur les données transmises par la Police grand-ducale et le Ministère public au ministre

i. Sur les données qui portent sur des faits n'ayant pas donné lieu à une décision de justice

- Ad paragraphes (2) et (3) de l'article 14 nouveau

Le paragraphe (2) de l'article 14 nouveau du projet de loi dispose que les informations relatives aux faits, visés au paragraphe (3) de l'article précité, sont communiquées au ministre « sous forme de l'intégralité ou d'extraits de procès-verbaux ou rapports de police, jugements, arrêts, ordonnances, ou tout autre document ou acte de procédure contenant les informations concernées ».

Le texte précise encore que « les faits auxquels se rapportent les informations fournies par le Ministère public et la Police grand-ducale ne peuvent avoir été commis plus de cinq ans avant l'introduction de la demande en obtention d'une autorisation, d'un permis ou d'un agrément prévus par la présente loi, sauf si ces faits ont fait l'objet d'une condamnation pénale ou font l'objet

d'une poursuite pénale en cours, auquel cas le délai de cinq ans est porté à 10 ans ».

S'il y a lieu de féliciter les auteurs du projet de loi pour ces précisions, le texte ne précise pas avec suffisamment de clarté :

- quelles seraient les données transmises par la Police grand-ducale au ministre, et sous quelles formes celles-ci seraient transmises ; et
- quelles seraient les données transmises par le Ministère public au ministre, et sous quelles formes celles-ci seraient transmises.

De telles précisions sont importantes alors que le ministre serait susceptible de recevoir plusieurs documents relatifs à des mêmes faits par la Police grand-ducale et le Ministère public. Or, pareille situation ne serait pas conforme au principe de minimisation des données.

En outre, la formulation « *tout autre document ou acte de procédure contenant les informations concernées* » est trop vague, de sorte qu'il n'est pas possible de comprendre à sa lecture quelles seraient les informations communiquées. Une telle formulation est source d'incertitudes et d'insécurité juridique²⁸ et des précisions mériteraient d'être apportées par les auteurs du projet de loi.

Par ailleurs, il est encore regrettable que les auteurs du projet de loi n'aient pas précisé quelles étaient les situations pour lesquelles il serait justifié de communiquer au ministre l'intégralité ou seulement un extrait des informations visées au dernier alinéa du paragraphe (2) article 14

²⁸ 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.

6

ANNEXES

nouveau du projet de loi alors que de telles explications sont apportées par les auteurs du projet de loi en ce qui concerne le paragraphe (5) de l'article précité.

En tout état de cause, des explications quant à la nécessité d'obtenir de telles informations devraient être fournies par les auteurs du projet de loi.

- Ad paragraphe (4) de l'article 14 nouveau

Dans l'hypothèse où une enquête préliminaire ou une instruction préparatoire est en cours, seules les données visées au paragraphe (4) de l'article 14 précité pourront être transmises au ministre. La Commission nationale se félicite de telles précisions.

En outre, et comme relevé par le Conseil d'Etat dans son avis complémentaire précité, quelle serait la portée du secret de l'instruction par rapport aux règles de la procédure administrative non contentieuse et contentieuse ?

ii. Sur les données qui portent sur des faits ayant donné lieu à une décision de justice

Il y a lieu de constater que le paragraphe (5) de l'article 14 nouveau prévoit que sur demande « le procureur d'Etat communique au Ministre copie des décisions judiciaires qui figurent le cas échéant sur le bulletin n°2 du casier judiciaire de la personne concernée, délivré au Ministre conformément à l'article 15, paragraphe 4 ».

Les auteurs du projet de loi précisent que « lorsque l'extrait n°2 du casier judiciaire du demandeur renseigne sur plusieurs condamnations pour des faits graves, parfois avec des peines d'emprisonnement fermes (...) la communication des jugements ou arrêts en cause n'est pas nécessaire, alors que la demande peut alors être refusée sur base du seul casier judiciaire. Cependant, lorsque l'extrait ne renseigne, par exemple, qu'une seule condamnation pour des coups et blessures volontaires, avec comme seule peine une amende, parfois même peu élevée, l'analyse des faits in concreto s'impose et la communication d'une copie du jugement ou de l'arrêt est alors nécessaire ».

La CNPD considère au vu des justifications des auteurs du projet de loi que le principe de minimisation des données pourrait être respecté dans de tels cas, alors que la communication de telles décisions ne serait pas systématique.

Néanmoins, il y a lieu de relever que l'alinéa 2 du paragraphe (2) de l'article 14 nouveau prévoit que les informations, concernant les faits visés au paragraphe (3), pourront être communiquées au ministre sous forme de l'intégralité ou d'extraits de « jugements, arrêts, ordonnances ».

Les auteurs du projet de loi ne justifient pas dans leur commentaire de l'article la nécessité et l'utilité d'une telle communication alors que le ministre peut, d'ores et déjà, avoir accès, le cas échéant, aux décisions qui figurent sur le bulletin n°2 de la personne concernée.

Ces dispositions visent-elles la possibilité pour le ministre d'obtenir des décisions qui ne seraient pas encore définitives ou non encore inscrites au bulletin n°2 ? Si tel devait être le cas, la Commission nationale partage les réserves émises par le Conseil d'Etat ainsi que le Parquet général dans leur avis respectif sur la transmission de décisions non définitives²⁹. Ne faudrait-il pas prévoir à l'instar de l'alinéa 2 du paragraphe (4) que le ministre a la possibilité de tenir en suspens une demande d'autorisation, d'agrément ou de permis pour les cas où une décision ne serait pas définitive ?

En tout état de cause, ce système ne devrait pas permettre au ministre d'obtenir la communication de décisions de justice qui n'apparaîtraient plus sur l'extrait de casier judiciaire pour les cas où une réhabilitation pénale aurait été accordée.

b. Sur l'échange de données entre le SRE et le ministre

i. Remarques liminaires

Les auteurs du projet de loi précisent dans leur commentaire du paragraphe (6) de l'article 14 nouveau que ce paragraphe prévoit la base légale qui permettrait au Service Armes & Gardiennage et au SRE d'échanger des informations qui seraient nécessaires à l'accomplissement de leurs missions respectives.

Cependant, il y a lieu de constater que l'échange de données, tel que prévu par le paragraphe

(6) de l'article précité, entre le ministre et le SRE dans le cadre de l'exécution de ses missions telles que visées à l'article 3, paragraphe (2) de la loi modifiée du 5 juillet 2016 portant réorganisation du SRE est déjà prévu par les dispositions des articles 9 et 10 de la loi précitée³⁰.

La Commission nationale se demande, dès lors, comment s'articulent les présentes dispositions avec les dispositions visées aux articles 9 et 10 de la loi modifiée du 5 juillet 2016 portant réorganisation du SRE.

ii. Sur les données communiquées par le SRE au ministre

Il y a lieu de relever que le paragraphe (6) de l'article 14 nouveau du projet de loi dispose que « *le Ministre et le Service de renseignement de l'Etat échangent (...) les informations qui sont nécessaires (...)* ».

Dans leur commentaire du paragraphe (6) de l'article 14 nouveau, les auteurs du projet de loi précisent qu'il est important de « *disposer de toutes les informations connues sur une personne afin de ne pas courir le risque de donner une autorisation en matière d'armes à un potentiel extrémiste à propension violente, voire un terroriste en puissance* ».

Or, eu égard à la nature des données qui seraient communiquées, il est impératif que des précisions soient apportées par les auteurs du projet de loi quant aux catégories de données qui

²⁹ Voir avis du parquet général, document parlementaire N°7425/02, page 18, commentaires sous le point 22) et avis du Conseil d'Etat, document parlementaire n°7425/04, page 23, commentaires relatifs à l'article 50.

³⁰ L'article 9, paragraphe (2) dispose que « [l]e SRE communique dans les meilleurs délais les renseignements collectés dans le cadre de ses missions aux autorités judiciaires, aux services de la police grand-ducale et aux administrations dans la mesure où ces renseignements paraissent utiles à l'accomplissement de leurs missions respectives », l'article 10, paragraphe (2) dispose que « [d]ans le cadre de l'exercice de sa mission, le SRE a accès direct, par un système informatique, aux traitements de données à caractère personnel suivants: (...) g) le fichier des armes prohibées du ministre ayant la Justice dans ses attributions ».

6

ANNEXES

seraient communiquées par le SRE au ministre afin de respecter le principe de prévisibilité et de précision auquel doit répondre tout texte légal ou réglementaire³¹.

En l'absence de telles précisions, la CNPD n'est pas en mesure d'apprécier si un tel traitement de données est susceptible de respecter le principe de minimisation des données.

Sur ce point, il est suggéré aux auteurs du projet de loi de s'inspirer des dispositions légales de la loi allemande du 17 février 2020 (« *Waffengesetz* ») qui précise les infractions sur lesquelles porte la vérification de la « *Zuverlässigkeit* » effectuée par l'équivalent du SRE allemand³².

c. Sur la transmission de données par les juridictions pénales d'un Etat membre au ministre

En ce qui concerne le paragraphe (8) de l'article 14 nouveau, les auteurs du projet de loi sous avis précisent dans leur commentaire y afférent qu'il ne s'agit pas de « *dispositions nouvellement proposées par les présents amendements* » mais qu'il s'agit en substance de la reprise du paragraphe (4) de l'article 57 initial du projet de loi.

Or, il y a lieu de relever que si ce paragraphe est une reprise fidèle du paragraphe (4) de l'article 57 initial du projet de loi, la CNPD est d'avis que l'apposition du terme « *[p]our les besoins de l'appréciation de l'honorabilité* » au début du paragraphe (8) de l'article 14 nouveau change le sens des dispositions initiales. Cela laisse, en effet, supposer que les condamnations à l'étranger sont à prendre compte lors de la vérification de l'honorabilité.

Si tel devait être le cas, l'origine des données devrait être précisée, de même que les catégories de données prises en compte par le ministre dans le cadre de la vérification d'honorabilité devraient être précisées. S'il devait s'agir de la communication des extraits de casiers judiciaires provenant d'un autre Etat membre de l'Union européenne, d'un pays associé à l'espace Schengen ou de l'Espace économique européen, alors cela devrait être reflété dans le dispositif.

2. Sur la mise en place d'un système de suivi en ce qui concerne la vérification de l'honorabilité

L'article 5 paragraphe (2) de la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE

³¹ 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.

³² Le paragraphe (5) paragraphe (5) intitulé « *Zuverlässigkeit* », point (5), 4., de la loi allemande du 17 février 2020 dispose que « (5) Die zuständige Behörde hat im Rahmen der Zuverlässigkeitsprüfung folgende Erkundigungen einzuholen: (...) 4. die Auskunft der für den Wohnsitz der betroffenen Person zuständigen Verfassungsschutzbehörde, ob Tatsachen bekannt sind, die Bedenken gegen die Zuverlässigkeit nach Absatz 2 Nummer 2 und 3 begründen; liegt der Wohnsitz der betroffenen Person außerhalb des Geltungsbereichs dieses Gesetzes, ist das Bundesamt für Verfassungsschutz für die Erteilung der Auskunft zuständig. Die nach Satz 1 Nummer 2 erhobenen personenbezogenen Daten dürfen nur für den Zweck der waffenrechtlichen Zuverlässigkeitsprüfung verwendet werden. Erlangt die für die Auskunft nach Satz 1 Nummer 4 zuständige Verfassungsschutzbehörde im Nachhinein für die Beurteilung der Zuverlässigkeit nach Absatz 2 Nummer 2 und 3 bedeutsame Erkenntnisse, teilt sie dies der zuständigen Behörde unverzüglich mit (Nachbericht). Zu diesem Zweck speichert sie Name, Vorname, Geburtsdatum, Geburtsname, Geburtsort, Wohnort und Staatsangehörigkeit der betroffenen Person sowie Aktenfundstelle in den gemeinsamen Dateien nach § 6 des Bundesverfassungsschutzgesetzes. Lehnt die zuständige Behörde einen Antrag ab oder nimmt sie eine erteilte Erlaubnis zurück oder widerruft diese, so hat sie die zum Nachbericht verpflichtete Verfassungsschutzbehörde hiervon unverzüglich in Kenntnis zu setzen. Die zum Nachbericht verpflichtete Verfassungsschutzbehörde hat in den Fällen des Satzes 5 die nach Satz 4 gespeicherten Daten unverzüglich zu löschen. ».

du Conseil relative au contrôle de l'acquisition et de la détention d'armes (ci-après la « directive ») prévoit un système de suivi « *qui fonctionne de manière continue ou périodique visant à garantir que les conditions d'octroi d'une autorisation fixées par le droit national sont remplies pour toute la durée de l'autorisation* ». Un tel système qui n'était pas transposé dans le projet de loi initial semble être transposé suite aux amendements sous avis.

En effet, la CNPD comprend qu'un système de suivi quant à la condition d'honorabilité serait instauré, tel que cela ressort des dispositions des paragraphes (4), alinéa 3, et (6) de l'article 14 nouveau ainsi qu'à l'article 51 (49 initial) du projet de loi. Elle entend préciser les points suivants quant à ces dispositions.

Par ailleurs, à défaut de précision dans le projet de loi sous avis, il y a lieu de s'interroger sur la mise en place pratique du système de suivi envisagé. En effet, dans la mesure où le Ministère public, la Police grand-ducale et le SRE ont accès au fichier des armes³³, tenu par le ministre, ces derniers consulteront ils ledit fichier de façon proactive et de manière régulière afin de faire remonter au ministre des informations susceptibles de remettre en cause « l'honorabilité » d'un titulaire d'une autorisation, agrément ou permis en cours de validité ?

A. Ad paragraphe (4) alinéa 3 de l'article 14 nouveau du projet de loi

L'alinéa 3 du paragraphe (4) de l'article susvisé précise que les données visées à l'alinéa 1 du

paragraphe (4) de l'article précité peuvent être communiquées par le procureur d'Etat général au ministre « *lorsqu'il dispose d'informations susceptibles de mettre en doute l'honorabilité* » d'un titulaire d'une autorisation, d'un permis ou d'un agrément en cours de validité.

Les dispositions de l'alinéa 1 du paragraphe (4) de l'article 14 nouveau du projet de loi énumèrent les données pouvant être communiquées dans le cas où une enquête préliminaire ou une instruction préparatoire est en cours pour les faits visés au paragraphe (3) de l'article 14 précité.

Cependant, il y a lieu de relever que le texte sous avis reste muet quant aux informations qui concerneraient des faits qui ne font pas l'objet d'une enquête préliminaire ou d'une instruction préparatoire.

Par ailleurs, la Commission nationale se demande comment le ministre obtient les « *informations susceptibles de mettre en doute l'honorabilité* » relatives à un titulaire d'une autorisation, d'un permis ou d'un agrément en cours de validité ? Est-ce que l'obtention de telles informations se fait par l'intermédiaire du Ministère public via la procédure visée à l'article 51 du projet de loi sous avis ? Qu'en est-il de la Police grand-ducale ou du SRE si ces derniers devaient disposer d'informations susceptibles de mettre en doute l'honorabilité d'un titulaire d'une autorisation, permis ou agrément en cours de validité ?

³³ Conformément à l'article 48-24 du Code de procédure pénale, à l'article 43 de la loi du 18 juillet 2018 sur la Police grand-ducale et à l'article 10 de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, les parquets, la Police grand-ducale et le SRE ont respectivement accès au fichier des armes.

6

ANNEXES

Des précisions à ce sujet mériteraient d'être indiquées par les auteurs du projet de loi.

B. Ad paragraphe (6) de l'article 14 nouveau du projet de loi

L'article 14 nouveau paragraphe (6) du projet de loi prévoit un échange entre le ministre et le SRE des informations nécessaires à l'appréciation de l'honorabilité. Il y a cependant lieu de constater que cette vérification de l'honorabilité n'est pas encadrée temporellement.

La CNPD recommande de préciser, à l'instar de la loi allemande du 17 février 2020, les modalités d'un tel échange notamment dans l'hypothèse où le SRE obtiendrait des informations, concernant un titulaire d'une autorisation, d'un permis ou d'un agrément en cours, qui seraient susceptibles d'avoir des conséquences sur son honorabilité.

C. Ad article 51 (49 initial) du projet de loi

L'amendement n°51 est une reformulation complète de l'article 51 (49 initial) du projet de loi. Cet article intitulé « Information du Ministre par le Ministère public » vise l'obtention d'informations par le Service Armes & Gardiennage de la part du Parquet de Luxembourg et non de la Police grand-ducale comme cela était prévu initialement dans l'article 49 du projet de loi. La transmission d'informations intervient si le « *procureur général d'Etat et le procureur d'Etat compétent estiment que la transmission du procès-verbal ou du rapport est opportune* ».

Bien que cela ne ressorte pas expressément du dispositif sous avis, la CNPD comprend que ce dispositif s'inscrit dans la mise en place d'un système de suivi afin que le ministre s'assure que le titulaire d'un agrément, d'une autorisation ou d'un permis en cours, délivré sur base du projet de loi, remplisse toujours la condition d'honorabilité visée à l'article 14 nouveau du projet de loi. Si les dispositions de cet article ne devaient pas viser une telle hypothèse, quelle serait, dès lors, la finalité et la nécessité d'une telle communication ?

Dans la mesure où cet article semble être le pendant de l'article 14 du projet de loi sous avis, il conviendrait de préciser que les informations concernant un fait commis par un titulaire d'une autorisation, d'un agrément ou permis ne puissent concerner que les faits visés au paragraphe (3) de l'article 14.

En effet, la formulation actuelle « *si le procureur général d'Etat et le procureur d'Etat compétent estiment que la transmission du procès-verbal ou du rapport est opportune* » apparaît trop vague aux yeux de la CNPD, dans la mesure où elle pourrait être interprétée comme élargissant les faits pouvant faire l'objet d'une vérification d'honorabilité.

Par ailleurs, ne faudrait-il pas également prévoir la communication de telles informations sous forme d'avis circonstancié du procureur général d'Etat ou du procureur d'Etat compétent plutôt que la transmission de procès-verbaux ou de rapports ?

3. Sur la durée de conservation des données obtenues dans le cadre de la vérification de l'honorabilité

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 dans le cadre de l'enquête administrative et dans le cadre du système de suivi. En l'absence de précisions des auteurs du projet de loi sur ce point, la CNPD n'est pas en mesure d'apprécier si, en l'occurrence, le principe de durée de conservation limitée des données est respecté.

Or, la Commission nationale estime essentiel que des précisions à ce sujet soient apportées et ce d'autant plus eu égard à la nature des données à caractère personnel en cause.

Ainsi, la durée de conservation devrait être définie dans le projet de loi ou celui-ci devrait au 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.

A titre d'exemple, il est suggéré aux auteurs du projet de loi de s'inspirer des dispositions françaises qui fixent une durée de conservation pour les données issues de l'enquête

administrative. L'article R312-88 du Code de la sécurité intérieure française dispose que : « *[[]es données à caractère personnel et informations mentionnées au d du 1° du I et aux V et VI de l'article R. 312-85 [les données issues de l'enquête administrative] sont conservées pendant une durée maximale d'un an à compter de la notification des décisions mentionnées au IV du même article ou, en cas de recours contentieux dirigé contre ces décisions, jusqu'à ce qu'il ait été définitivement statué sur le litige* ».

Enfin, il y a également lieu de constater que le dispositif sous avis ne prévoit aucune disposition relative à la mise à jour des données obtenues par le ministre dans le cadre de la vérification d'honorabilité. Or, compte tenu des données collectées, il convient d'attirer l'attention des auteurs du projet de loi sur le fait qu'il existe un risque important que des données relatives à une personne dont l'affaire a été classée sans suite ou qui a entretemps été acquittée d'une infraction dont elle a été accusée se trouvent toujours dans les dossiers de l'administration, sans une mise à jour ou rectification afférente.

4. Sur le droit des personnes concernées

Selon l'article 5 paragraphe (1) lettre (a) du RGPD, les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (principe de licéité, loyauté, transparence), ce qui implique notamment que le ministre devra respecter les dispositions de l'article 13 du RGPD pour ce qui de la

6

ANNEXES

collecte de données directement auprès de la personne concernée, sinon celles de l'article 14 du RGPD, lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée elle-même, c'est-à-dire celles collectées indirectement auprès du Ministère public, de la Police grand-ducale ou du SRE. En vertu de ces articles, le responsable du traitement fournit à la personne concernée des informations au sujet du traitement la concernant, notamment pour garantir un traitement équitable et transparent.

Dès lors, dans la mesure où le ministre, dans le cadre de l'enquête administrative, ne collecte pas directement les données auprès des personnes concernées celui-ci doit fournir l'ensemble des informations visées à l'article 14 du RGPD. Ces informations devront être fournies à la personne concernée au plus tard un mois après que le ministre ait obtenu les données.

Enfin, il y a lieu d'attirer l'attention des auteurs du projet de loi sur le fait que sans dérogation explicite dans le projet de loi, ces droits sont tous applicables intégralement. Or, de telles dérogations pourraient s'avérer opportunes lorsque les informations obtenues dans le cadre de la vérification d'honorabilité concernent des enquêtes ou instructions pénales en cours.

A toutes fins utiles, il y a lieu de préciser que la législation française en matière d'armes prévoit, à l'article R.312-90 du Code de la sécurité intérieure, une restriction des droits des personnes concernées. Cet article dispose notamment que : « [l]es droits d'information,

d'accès, de rectification et à la limitation des données mentionnés aux articles 13 à 16 et 18 du [RGPD] et aux articles 104 à 106 de la loi du 6 janvier 1978 précitée s'exercent auprès du service central des armes ou du préfet territorialement compétent, en fonction de leurs attributions respectives. Afin d'éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires ou d'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 ou de protéger la sécurité publique, les droits d'accès, de rectification et à la limitation peuvent faire l'objet de restrictions en application de l'article 52 et des 2° et 3° du II et du III de l'article 107 de la loi du 6 janvier 1978 précitée. ».

5. Sur l'autorité de contrôle compétente

Il y a lieu de s'interroger sur le fait de savoir quelle est l'autorité de contrôle compétente pour contrôler et surveiller le respect des dispositions légales prévues par l'article 14 nouveau du projet de loi, en l'absence de précision dans le projet de loi sous avis.

En effet, il existe un doute sur le point de savoir si les données, collectées initialement pour les besoins de la prévention, de la recherche, de la constatation et de la poursuite des infractions, puis transmises par la Police grand-ducale, le Ministère public et le SRE au ministre afin de lui permettre de vérifier l'honorabilité d'un demandeur de permis, autorisation ou agrément visés par le projet de loi relève de la compétence

de l'autorité de contrôle judiciaire³⁴ ou de celle de la Commission nationale.

Il y a lieu de rappeler que le paragraphe (2) de l'article 40 de la loi du 1^{er} 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 dispose que « *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, que ce soit pour les finalités visées à l'article 1er de la présente loi ou pour celles visées par le [RGPD], sont soumises au contrôle de l'autorité de contrôle judiciaire* ».

Les auteurs du projet de loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale estiment que « *pour déterminer la compétence d'une des deux autorités de contrôle [CNPD ou autorité de contrôle judiciaire], la question déterminante ne sera plus la finalité de la donnée concernée, mais celle de savoir si l'autorité compétente participe à la prise ou à l'exécution d'une décision juridictionnelle, ce qui n'est pas le cas pour la Police* »³⁵.

Ils précisent encore que « *lorsque pour un traitement de données à caractère personnel déterminée – relevant du champ d'application du présent projet de loi – la question de la compétence d'une des deux autorités de contrôle se pose, il faudrait en principe retenir la*

compétence de la Commission nationale pour la protection des données, sauf si le traitement de données à caractère personnel concerné est effectué par une juridiction dans l'exercice de ses fonctions juridictionnelles ou par le ministère public, soit dans l'exercice de ses fonctions juridictionnelles, soit en amont ou en aval de sa participation à la prise d'une décision juridictionnelle »³⁶.

En l'espèce, le ministère de la Justice n'est pas une des autorités visées par l'article 40 de la loi de la loi du 1^{er} 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 ne rendra pas une décision juridictionnelle à l'issue de l'enquête administrative mais une décision purement administrative (par exemple délivrance d'une autorisation pour le port d'armes).

Dès lors, le traitement de données effectué par le ministre dans le cadre de l'enquête administrative, visée par l'article 14 nouveau du projet de loi, pourrait tomber dans le champ de compétence de la Commission nationale.

Il est intéressant de noter que cette solution a été retenue en ce qui concerne l'autorité compétente pour surveiller et contrôler les dispositions de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière³⁷.

Dans un souci de sécurité juridique et de lever tout équivoque sur ce point, les auteurs du

³⁴ Autorité de contrôle de judiciaire telle que visée par l'article 40 de la loi du 1^{er} 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.

³⁵ Voir document parlementaire n°7168, « *Ad article 41* », page 47.

³⁶ Voir document parlementaire n°7168, « *Ad article 41* », page 47.

³⁷ Articles 25, paragraphe (1), et 28 de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière.

6

ANNEXES

projet de loi devrait compléter le dispositif sous avis en conséquence.

A toutes fins utiles, il y a lieu de relever que la compétence de la CNPD en ce qui concerne les traitements de données effectués par le ministre dans le cadre du projet de loi sous avis ne préjuge en rien de la compétence de l'autorité de contrôle judiciaire en ce qui concerne la communication de données par le Ministère public au ministre en application de l'article 14 nouveau du projet de loi.

6. Remarques finales

Il y a lieu de relever que dans son avis complémentaire du 19 décembre 2020 le Conseil d'Etat³⁸ propose d'omettre la notion d'honorabilité au profit du critère de dangerosité. En effet, le Conseil d'Etat estime que le critère de l'honorabilité est « *difficilement transposable à la vérification de l'aptitude d'une personne à détenir ou à manier une arme* ». *La haute autorité se demande encore si « le seul motif pour refuser une autorisation, un permis ou un agrément ne devrait pas consister dans la dangerosité du demandeur. En effet, le critère d' « honorabilité » apparaît uniquement dans les réglementations relatives à l'accès à une profession et à l'exercice de celle-ci. »*

Cependant, comme relevé par le Conseil d'Etat le projet de loi se réfère « au concept d' « honorabilité » dans le cadre de deux appréciations différentes, celle des armuriers et courtiers, sous l'acception de l'honorabilité dite professionnelle, et celle des particuliers, sous la forme de l'honorabilité personnelle ».

La CNPD se rallie à l'avis du Conseil d'Etat uniquement en ce qu'il n'est pas pertinent d'utiliser la notion d' « honorabilité » pour apprécier si un particulier dispose de l'aptitude requise pour détenir ou manier une arme. Néanmoins, la référence à la notion d' « honorabilité » pourrait apparaître pertinente en ce qui concerne les agréments qui seraient délivrés par le ministre aux armuriers ou courtiers. Lesdits agréments étant un prérequis à l'accès de telles professions.

A ce titre, il est précisé qu'en France la notion d' « honorabilité » est utilisée pour toute personne souhaitant « *exercer l'activité qui consiste, à titre principal ou accessoire, soit en la fabrication, le commerce, l'échange, la location, la location-vente, le prêt, la modification, la réparation ou la transformation, soit en la négociation ou l'organisation d'opérations en vue de l'achat, de la vente, de la fourniture ou du transfert d'armes, de munitions ou de leurs éléments* »³⁹. Cependant cette notion n'est pas reprise pour les personnes souhaitant acquérir ou détenir une arme, en effet, l'article L.312-3-1 du Code de la sécurité intérieure français dispose que « *[l']autorité administrative peut interdire l'acquisition et la détention des armes, munitions et de leurs éléments des catégories A, B et C aux personnes dont le comportement laisse craindre une utilisation dangereuse pour elles-mêmes ou pour autrui* ».

La Commission nationale reviendra plus en détail sur la référence faite à la notion d'honorabilité dans la législation luxembourgeoise dans son avis sur le projet de loi n°7691, qui vise à harmoniser et préciser les différentes

³⁸ Voir document parlementaire n°7425/08, commentaires relatifs à l'amendement 14, page 7.

³⁹ Article L.313-2 du Code de la sécurité intérieure français.

procédures de « contrôle d'honorabilité » actuellement prévues dans plusieurs textes de lois.

Par ailleurs, comme relevé par le Conseil d'Etat. Il faudra veiller à prendre en compte les avis formulés à l'encontre du projet de loi sous avis alors que le projet de loi n°7691 entend modifier l'article 16, de la loi modifiée du 15 mars 1983 sur les armes et munitions, qui sera abrogé par le projet de loi sous avis. Or, le dispositif proposé est identique à celui prévu par l'article 14 nouveau du projet de loi.

2. Sur le fichier des armes

L'amendement n°15 vise à modifier l'article 13 initial du projet de loi concernant le fichier des armes tenu par le ministre.

La Commission nationale accueille favorablement les amendements apportés par les auteurs du projet de loi aux paragraphes (1), (2) et (4) de l'article 15 (13 initial) du projet de loi sous avis qui tiennent compte des remarques formulées par la Commission nationale dans son avis du 8 juillet 2019 et par le Conseil d'Etat dans son avis du 12 juillet 2019.

Néanmoins, il est regrettable que les auteurs du projet de loi n'aient pas précisé quelles catégories de données seraient traitées et pour quelles finalités, tel que cela avait été soulevé par la CNPD dans son avis précité, alors qu'il ressort désormais du paragraphe (1) de l'article précité que le traitement de données effectué par le ministre poursuit plusieurs finalités.

Par ailleurs, si les données collectées et traitées dans le cadre de l'enquête administrative sont amenées à figurer dans ce fichier alors cela devrait ressortir clairement de cet article.

A titre d'exemple, il est suggéré aux auteurs du projet de loi de prendre exemple sur la structure de l'article R.312-85 du Code de la sécurité intérieure français qui précise les différentes catégories de données à caractère personnel pouvant être collectées par le ministre de l'intérieur (service central des armes) dans le cadre de la mise en œuvre du traitement automatisé de données à caractère personnel dénommé « système d'information sur les armes » pour les finalités précisées à l'article R.312-84 du Code de la sécurité intérieure.

Ainsi, cet article regroupe six grandes catégories différentes à savoir :

- Les données d'identification des acquéreurs et détenteurs d'armes et de leurs éléments ;
- Les données d'identification des armes et éléments d'armes ;
- Les données d'identification des personnes se livrant à la fabrication, au commerce ou à l'intermédiation d'armes ;
- Les données relatives à la délivrance des titres d'acquisition, de détention, de port, de fabrication, de commerce et d'intermédiation des armes, des munitions et de leurs éléments ;
- Les données et informations issues de l'enquête administrative ;
- Les catégories particulières de données qui seraient en cas de nécessité absolue collectées.

6

ANNEXES

1. Ad paragraphe (3) de l'article 15 (13 initial) du projet de loi

Ce paragraphe prévoit l'accès à certaines autorités nationales aux informations visées au paragraphe (2) de l'article 15 (13 initial) du projet de loi. Il s'agirait donc d'un accès restreint au fichier des armes puisque la CNPD comprend que figurent également dans ce fichier l'ensemble des « *documents gérés aux fins de l'exécution de la présente loi* ».

Or, un accès général au fichier des armes prohibées au sens de la loi modifiée du 15 mars 1983 sur les armes et munitions (fichier des armes au sens du projet de loi) est prévue pour :

- les parquets conformément aux dispositions de l'article 48-24 du Code de procédure pénale ;
- la Police grand-ducale conformément à l'article 43 de la loi du 18 juillet 2018 sur la Police grand-ducale ; et
- le SRE conformément à l'article 10 de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat.

Dès lors et tel que relevé par le Conseil d'Etat dans son avis en date du 12 juillet 2019, les auteurs du projet de loi devraient préciser dans quelle mesure les dispositions du paragraphe (3) de l'article 15 (13 initial) du projet de loi s'articulent avec de telles dispositions.

En l'absence de précision sur ce point ainsi qu'aux modalités de l'accès prévu au paragraphe (3) de l'article 15 (13 initial) du projet de

loi, la Commission nationale peut difficilement apprécier sa conformité au RGPD et déplore que de telles précisions n'aient pas été apportées.

En outre, celle-ci s'interroge sur la possibilité que d'autres administrations, autres celles compétentes pour « *la prévention, la recherche et la constatation des infractions pénales* », aient accès aux données issues de l'enquête administrative. Ce point devrait être clarifié par les auteurs du projet de loi.

Pour le surplus en ce qui concerne ce paragraphe, la Commission nationale réitère ses observations formulées à ce sujet dans son avis du 8 juillet 2019.

Enfin, en ce qui concerne la suppression de la première phrase du dernier alinéa du paragraphe (3) de l'article 15 (13 initial du projet de loi), la CNPD regrette une telle suppression alors que la phrase prévoyait que « *les données à caractère personnel devaient être effacées du fichier à l'issue des périodes visées à l'alinéa 2* ». Elle rappelle à ce titre qu'au-delà de la durée de conservation des données déterminée par le responsable du traitement, les données doivent être supprimées ou anonymisées.

2. Ad paragraphe (5) de l'article 15 (13 initial) du projet de loi

Les dispositions nouvelles du paragraphe (5) de l'article 15 (13 initial) du projet de loi énumèrent les catégories de données « *pouvant faire l'objet d'un échange* » entre le ministre et

les autorités nationales et étrangères dans la mesure où « ces échanges ont comme finalité l'exécution de la présente loi et de ses règlements d'exécution ou d'une des dispositions légales visées aux points 1° et 2° ».

Il y a lieu de relever que la formulation actuelle du texte en ce qui concerne les finalités des échanges est rédigée de manière trop vague et n'est pas conforme au principe de précision et de prévisibilité auquel doit répondre un texte de loi conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme⁴⁰. De plus, si la Commission nationale se félicite que les catégories de données sur lesquelles portent les échanges soient énumérées dans le projet de loi, il conviendrait néanmoins de préciser quelles catégories de données seraient susceptibles d'être communiquées à quelle autorité et pour quelle finalité.

En l'absence de telles précisions, la CNPD n'est pas en mesure d'apprécier si les échanges de données visés par le paragraphe (5) de l'article 15 (13 initial) respectent les principes de minimisation des données et de limitation des finalités.

Par ailleurs, faut-il prévoir un échange de données entre le ministre et les autorités nationales compétentes pour « *la prévention, la recherche et la constatation des infractions pénales* » alors que cela semble être déjà prévu par le paragraphe (3) de l'article 15 du projet de loi sous examen (voir nos développements sous le point 3) i. du présent avis).

Enfin, en ce qui concerne les échanges de données avec des autorités étrangères, la Commission nationale réitère ses observations formulées dans son avis du 8 juillet 2019.

3. Sur l'attestation médicale

L'amendement n°16 modifie l'article 14 initial du projet de loi relatif à l'attestation médicale devant être communiquée par le requérant dans le cadre de sa demande de permis, agrément ou autorisation.

La Commission nationale salue les précisions apportées au paragraphe (1) de l'article 16 (14 initial) du projet de loi.

Néanmoins, la CNPD regrette que le paragraphe (4) de l'article 16 (14 initial) du projet de loi ne précise pas les catégories de données à caractère médical et psychologique qui seraient obtenues par le ministre après que celui-ci ait octroyé un permis ou une autorisation à un requérant, de même qu'elle déplore que l'origine de telles données ne soient pas précisées.

S'agit-il d'informations qui seraient obtenues dans le cadre de la procédure visée à l'article 51 du projet de loi et notamment en ce qui concerne les cas visés à l'article 71 du code pénal ? Est-ce que de telles informations sont obtenues par le ministre auprès des médecins qui auraient délivré l'attestation médicale visée au paragraphe (1) de l'article 16 (14 initial) du projet de loi ?

Des précisions quant à l'origine des données mériteraient donc d'être indiquées par les

⁴⁰ 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.

6

ANNEXES

auteurs du projet de loi. Ce d'autant plus que de telles données constituent des catégories particulières de données dites « données sensibles » au sens de l'article 9 du RGPD. Il est rappelé que pour le traitement de données à caractère personnel envisagé, le droit luxembourgeois doit prévoir « des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée ». Or, la formulation actuelle ne permet pas à la Commission nationale d'apprécier si tel est le cas.

4. Sur le registre des armes

L'amendement n°21 vise à modifier l'article 19 initial du projet de loi relatif au registre des armes. La Commission nationale salue que le paragraphe (3) de l'article 21 (19 initial) du projet de loi prévoit désormais que le registre des armes est remis au ministre en cas de cessation de l'activité de l'armurier. Néanmoins, la CNPD regrette que la durée de conservation dudit registre par l'armurier, qui permettait d'assurer une certaine prévisibilité juridique, ait été supprimée.

En outre, il y a lieu de relever que le dispositif ne prévoit pas non plus la durée de conservation du registre précité par le ministre en cas de remise par l'armurier si celui-ci cesse son activité. En l'absence de telles précisions la Commission nationale n'est pas en mesure d'apprécier si le principe de limitation de la conservation est respecté.

Il y a lieu de constater que le paragraphe (4) de l'article 21 (19 initial) du projet de loi a également

été amendé par les auteurs du projet. Le dispositif ne prévoit plus « une connexion électronique » mais un « système de transmission de données et informations par une voie électronique ». Bien que la CNPD se félicite que le terme « connexion électronique » ait été supprimé, elle regrette le manque de précisions du dispositif et réitère sur ce point ses observations formulées dans son avis du 8 juillet 2019.

5. Sur l'autorité de contrôle compétente en cas d'accès par les agents de l'Administration des douanes et accises au fichier des armes

L'amendement n°55 vise à modifier l'article 52 initial du projet de loi. La CNPD salue que les auteurs du projet de loi aient supprimé la référence faite au fichier des armes prohibées suite à sa recommandation formulée dans son avis du 8 juillet 2019.

Les modifications apportées au paragraphe (6) de l'article 54 (52 initial) du projet de loi consistent en une reformulation de l'autorité de contrôle compétente en matière de protection des données en ce qui concerne le contrôle des dispositions de l'article précité.

A ce titre, compte tenu des observations émises par le Conseil d'Etat dans son avis du 12 juillet 2019, il y a lieu de relever que l'Administration des douanes et accises, en règle générale, est chargée de missions à finalité fiscale mais est également chargée de certaines missions à finalité policière, comme par exemple en matière de drogues où certains douaniers disposent de

la qualité d'officier de police judiciaire. Pour les missions fiscales, le traitement de données à caractère personnel doit donc être fait suivant les dispositions du RGPD, tandis que les dispositions 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 s'appliquent au traitement de données à caractère personnel relevant des missions policières⁴¹.

En vertu du paragraphe (3) de l'article 54 (52 initial) du projet de loi, les fonctionnaires de l'Administration des douanes et accises ont la qualité d'officiers de police judiciaire dans l'exercice de leurs fonctions prévues au présent article. Dès lors, la formulation initiale du paragraphe (6) (paragraphe (7) initial) était exacte. Cependant, les modifications apportées au paragraphe (6) font désormais référence à la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, il est dès lors recommandé de se référer à la formulation qui avait été initialement employée par les auteurs du projet de loi.

En tout état de cause, il serait incorrect de considérer que l'autorité de contrôle

visée à l'article 40 de la loi du 1^{er} 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 pourrait être compétente alors que celle-ci n'est compétente que pour « *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* ». Or, tel n'est pas le cas en l'espèce.

Ainsi décidé à Belvaux en date du 4 février 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

⁴¹ Document parlementaire 7168/00, page 34, paragraphe 2.

6

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7691 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. (Délibération n°3/AV3/2021 du 10/02/2021)

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 1^{er} 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 12 novembre 2020, Madame la Ministre de la Justice a invité la Commission nationale à se prononcer sur le 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 (ci-après le « projet de loi »).

Selon l'exposé des motifs « [l]e projet de loi a pour objet de préciser les différentes procédures de « contrôle d'honorabilité » actuellement prévues dans plusieurs textes de loi relevant de la compétence du ministre de la Justice. ». Le « contrôle d'honorabilité » s'avère, par exemple, nécessaire dans le cadre du recrutement du personnel judiciaire ou encore dans le cadre de la délivrance d'une demande d'autorisation, de permis ou d'agrément en matière d'armes.

Dans ce contexte, les auteurs du projet de loi précisent que « certaines administrations et services de l'Etat ont besoin de connaître des informations parfois soumises au secret d'instruction ou considérées comme sensibles au vu des nouvelles règles relatives au traitement

des données » et qu' « [à] cet effet, le Ministère public doit pouvoir être saisi de demandes d'administrations ou de services exerçant une prérogative de puissance publique afin de se voir communiquer des informations relatives aux procédures pénales ou la délivrance de copie de pièces qui en sont issues ».

Comme le soulèvent les auteurs du projet de loi, le « contrôle d'honorabilité » vise à permettre aux administrations de l'Etat d'instruire « une demande en vue de l'octroi ou du refus d'une autorisation ». Ces dernières lorsqu'elles instruisent de telles demandes « doivent se baser sur des faits établis à suffisance de droit, et des rapports ou procès-verbaux établis par des officiers de police judiciaire », qui « sont une source reconnue à cette fin par la jurisprudence administrative ».

Selon l'exposé des motifs, le projet de loi précise « les finalités des traitements effectués dans le cadre des différentes procédures de vérification d'antécédents, en délimitant la consultation aux données essentielles et nécessaires et en déterminant la durée de conservation des données consultées par les autorités compétentes ». Les auteurs du projet de loi indiquent encore que l'objectif du projet de loi est « de permettre à toute personnes concernée par un traitement de données à des fins de contrôle d'honorabilité, de comprendre quels sont les différents types de données consultés et pour quels types d'objectifs ».

De telles vérifications des antécédents ou « contrôle d'honorabilité » ont indéniablement

6

ANNEXES

des répercussions sur le respect de la vie privée et la protection des données, la Commission nationale formulera ci-après ses observations quant aux problématiques soulevées à cet égard par les dispositions du projet de loi sous avis.

I. Introduction

1. Sur la notion d'honorabilité

En droit luxembourgeois, la notion d'honorabilité est « polysémique et fonction des matières et des finalités pour lesquelles il y est fait référence »⁴². Il n'est pas rare de constater que la référence faite à la notion d'« honorabilité » se retrouve sous des formulations différentes. En effet, certaines dispositions légales nationales font état de « conditions d'honorabilités à respecter », de « garanties d'honorabilité à respecter » ou encore de conditions ou garanties de « moralité » à respecter »⁴³. Les auteurs du projet de loi utilisent d'ailleurs également, dans l'exposé des motifs, tantôt le terme de « vérification des antécédents » tantôt celui de « contrôle d'honorabilité »⁴⁴.

Tel que relevé par le Conseil d'Etat, le concept de l'honorabilité « est essentiellement utilisé pour déterminer les conditions d'accès à une profession, souvent en rapport avec des notions telles que « moralité », « honorabilité professionnelle », « bonne réputation » et « activités irréprochables ». Afin de déterminer l'honorabilité professionnelle, les lois en cause visent, à côté des antécédents judiciaires, d'autres critères, souvent définis négativement, comme l'absence de l'accumulation de dettes

importantes auprès de créanciers publics ou l'usage dans le cadre de la demande d'autorisation de documents ou de déclarations falsifiées ou mensongers, l'absence de faillite, l'absence de condamnation pénale, etc. »⁴⁵.

Selon l'exposé des motifs du projet de loi, l'absence de définition commune de la notion d'honorabilité se justifie par la « diversité des matières qui recourent à une telle procédure et en conséquence les grandes différences dans les degrés d'ingérence qu'ils opèrent ».

S'il peut s'avérer difficile de trouver une définition commune eu égard à la diversité des matières et des procédures de vérification des antécédents ou de « contrôle d'honorabilité » y afférents, l'emploi de termes différents implique que chaque notion a une signification qui lui est propre.

Si tel ne devait pas être le cas, ne serait-il pas préférable d'utiliser la même terminologie plutôt que de continuer à utiliser par exemple les termes « moralité », « honorabilité professionnelle », « bonne réputation » ou « activités irréprochables » ?

Bien qu'il soit regrettable que le projet de loi sous avis ne propose pas de définition commune de la notion d'honorabilité ou n'emploie pas la même terminologie, il y a lieu de constater que celui-ci encadre toutefois les enquêtes diligentées à cet égard.

2. Sur le cadre légal instauré par le projet de loi

⁴² V. avis complémentaire du Conseil d'Etat du 19 décembre 2020 relatif au projet de loi N°7425 sur les armes et munitions, document parlementaire n°7425/08, développements sous « Amendement 14 ».

⁴³ V. exposé des motifs du projet de loi, page 5.

⁴⁴ Il s'agit des termes utilisés par les auteurs du projet de loi dans l'exposé des motifs, page 4.

⁴⁵ V. avis complémentaire du Conseil d'Etat du 19 décembre 2020 relatif au projet de loi N°7425 sur les armes et munitions, document parlementaire n°7425/08, développements sous « Amendement 14 ».

Le projet de loi instaure un cadre légal en ce qui concerne les vérifications d'antécédents ou de « *contrôle d'honorabilité* » devant être effectués dans le cadre des lois visées par le texte en projet.

Les auteurs du projet de loi précisent dans l'exposé des motifs qu'un tel cadre légal s'est avéré nécessaire car « *dans nombre de cas, la loi manque de définir précisément sur quels éléments portent la vérification d'antécédents ou le « contrôle d'honorabilité » ou quelles données sont prises en compte dans le cadre d'une telle procédure. En effet, les textes actuels ne permettent ainsi pas aux candidats ou requérants de savoir exactement quelles données les concernant sont consultées par les autorités compétentes* ».

Il ressort dudit projet de loi que les enquêtes diligentées aux fins de vérifier les antécédents peuvent être classées en trois catégories selon leur degré d'intrusion, quant à la vérification des antécédents judiciaires en fonction des agréments, permis, autorisations à délivrer selon le projet de loi ou des postes à pourvoir, tels que visés par le projet de loi.

En effet, la première catégorie de procédures regroupe les vérifications d'antécédents qui se basent sur la communication d'un extrait de

casier judiciaire (ci-après les « procédures de vérification des antécédents de type 1 »)⁴⁶.

La seconde catégorie de procédures regroupe les vérifications d'antécédents qui portent sur la communication d'un extrait de casier judiciaire, sur les faits relatifs à une condamnation pénale pour crime ou délit et pour laquelle la réhabilitation n'est pas déjà atteinte au moment de l'introduction de la demande, et sur les faits susceptibles de constituer un crime ou délit ayant donné lieu à l'établissement d'un procès-verbal de police, si ces faits font l'objet d'une poursuite pénale en cours, à l'exclusion des faits ayant abouti à une décision de non-lieu ou de classement sans suites (ci-après les « procédures de vérification des antécédents de type 2 »)⁴⁷.

La troisième catégorie de procédures concerne les vérifications d'antécédents qui portent sur la communication d'un extrait de casier judiciaire, les procès-verbaux et rapports de police concernant le requérant pour des faits qui ont fait l'objet d'une condamnation pénale ou incriminés en tant crime ou délit par la loi, visés à l'article 563, point 3° du Code pénal relatif aux voies de fait et violences légères, visés à l'article 1^{er} de la loi modifiée du 8 septembre 2003 sur la violence domestique (ci-après les « procédures de vérification des antécédents de type 3 »)⁴⁸.

⁴⁶ V. articles 1 relatif du projet de loi relatif à l'article 8-1 du Code de procédure pénale, article 2-3° du projet de loi relatif à l'article 1251-3 du Nouveau Code de procédure civile et article 13 du projet de loi relatif à l'article 2 de la loi du 6 mai 1999 relative à la médiation pénale, article 3 du projet de loi relatif à l'article 1^{er} de la loi modifiée du 7 juillet 1971 portant en matière répressive et administrative, institution d'experts, de traducteurs et d'interprètes assermentés

⁴⁷ V. article 4 du projet de loi relatif à l'article 16 de la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat, article 5 du projet de loi relatif à l'article 11 paragraphe (3) de la loi modifiée du 20 avril 1977 sur les jeux de hasard et les paris sportifs, article 6 du projet de loi relatif aux articles 76 et 77 de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire, article 7 du projet de loi relatif à l'article 90 bis de la loi modifiée du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif, article 11 du projet de loi relatif aux articles 2 et 3 de la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice et article 15 du projet de loi relatif à l'article 2 de la loi modifiée du 7 juin 2012 sur les attachés de justice.

⁴⁸ V. article 5 du projet de loi relatif à l'article 11 paragraphe (2) de la loi modifiée du 20 avril 1977 sur les jeux de hasard et les paris sportifs, article 9 du projet de loi relatif à l'article 16 de la loi modifiée du 15 mars 1983 sur les armes et munitions, article 12 du projet de loi relatif à l'article 3 de la loi du 31 janvier 1988 portant agrément des services d'adoption et définition des obligations leur incombant et de l'article 14 du projet de loi relatif à l'article 8bis de la loi du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance.

6

ANNEXES

Il y a lieu de regretter que ces trois procédures ne soient pas plus uniformisées en ce qui concerne les acteurs qui diligentent les enquêtes administratives et en ce qui concerne les modalités de transmission des informations issues de telles enquêtes.

En effet, il y a lieu de relever que soit le Ministère public diligente lui-même les enquêtes administratives⁴⁹ soit il communique les informations, nécessaires à l'enquête administrative, au ministre de la Justice⁵⁰ ou ministre des Finances⁵¹. Un schéma identique n'est donc pas reproduit pour l'ensemble des procédures.

De plus, il y a lieu de relever que lorsque le Ministère public diligente les enquêtes administratives, celui-ci rend à l'issue de celles-ci un avis, dont les éléments du contenu ne sont pas détaillés par le texte en projet. Lorsque le ministre de la Justice ou le ministre des Finances diligentent les enquêtes administratives ceux-ci se voient transmettre par le Ministère public les informations visées par le projet de loi. La CNPD y reviendra *infra* au point VI. du présent avis.

Ainsi, nonobstant la diversité des matières, il y a lieu de regretter qu'une structure commune n'ait pu être dégagée par les auteurs du projet de loi, en ce qui concerne les entités qui diligentent les enquêtes administratives et les modalités de transmission des données issues de telles enquêtes.

3. Sur le cadre légal en France

A titre de comparaison avec le système proposé par le texte sous avis, il est intéressant de

noter qu'il existe un cadre légal commun, en droit français, en ce qui concerne les enquêtes administratives ayant pour objet de vérifier les antécédents d'une personne souhaitant accéder à certaines professions ou sollicitant certaines autorisations ou certains agréments. Le système français repose sur les articles L.114-1 et L.234-1 du Code de la sécurité intérieure français (ci-après le « CSI ») qui fixent le cadre général des enquêtes administratives puis les modalités de ces enquêtes sont complétées par décrets.

L'article L.114-1 du CSI dispose que « *[l]es décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux, 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* ». Les articles R.114-2 à R.114-5 du CSI énumèrent les professions ou agréments qui peuvent donner lieu aux enquêtes mentionnées à l'article L.114-1 du CSI.

⁴⁹ V. articles 4, 6, 7, 11, 12 et 15 du projet de loi.

⁵⁰ V. articles 5, 9 et 14 du projet de loi.

⁵¹ V. article 5 du projet de loi.

A titre d'exemple, il y a lieu de relever que peut donner lieu à de telles enquêtes les « *personnes physiques employées pour participer à une activité privée de surveillance et de gardiennage* »⁵², le « *[r]ecrutement des membres des juridictions administratives, des magistrats de l'ordre judiciaire et des juges de proximité* »⁵³ ainsi que les décisions relatives à l'autorisation de « *pratiquer les jeux d'argent et de hasard dans les casinos autorisés* »⁵⁴, les décisions relatives à l'agrément des « *directeurs et des membres des comités de direction des casinos autorisés ainsi que des personnes employées dans les salles de jeux des casinos* »⁵⁵ ou encore les autorisations ou agréments relatifs à l'« *[a]cquisition, détention, fabrication, commerce, intermédiation, importation, exportation, transfert et transit de matériels de guerre, d'armes, de munitions et de leurs éléments de toute catégorie ; utilisation, exploitation, exportation et transit de matériels de guerre et matériels assimilés (...)* »⁵⁶.

Les articles L.234-1, R.234-1 du CSI viennent préciser les fichiers qui seront consultés lors d'une enquête administrative visée par l'article L.114-1 du CSI, ainsi que les modalités d'accès à de tels fichiers.

Il est encore intéressant de noter que ces enquêtes administratives sont diligentées par

le service national des enquêtes administratives de sécurité⁵⁷ (ci-après le « SNEAS ») et qu'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCRéD) permet au SNEAS de procéder à la consultation automatique et, le cas échéant, simultanée de traitements de données à caractère personnel pour vérifier si la personne concernée y est enregistrée⁵⁸.

Si les auteurs du projet de loi ont fait le choix de ne pas s'inspirer de l'approche française, c'est-à-dire, prévoir un cadre légal commun, la Commission nationale se demande s'il ne serait toutefois pas pertinent que les enquêtes administratives soient diligentées par une même et seule autorité à l'instar du SNEAS français et que seuls des avis rendant compte des résultats de l'enquête soient communiqués aux autorités concernées.

Par ailleurs, il est recommandé aux auteurs du projet de loi de s'inspirer de certaines dispositions françaises notamment en ce qu'elles énumèrent les fichiers qui pourront être consultés lors des enquêtes administratives, ainsi que les catégories de données à caractère personnel qui seraient collectées lors de telles enquêtes pour le cas où les données issues de telles enquêtes seraient conservées⁵⁹.

⁵² Article R.114-2, 1^o, c) du CSI

⁵³ Article R.114-2, 2^o du CSI

⁵⁴ R.114-3, 1^o, a) du CSI

⁵⁵ Article R.114-3, 2^o, a) du CSI

⁵⁶ Article R.114-5, 1^o du CSI

⁵⁷ V. décret n° 2017-668 du 27 avril 2017 portant création d'un service à compétence nationale dénommé « service national des enquêtes administratives de sécurité ».

⁵⁸ V. Décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCRéD).

⁵⁹ V. articles R.236-1 et suivants et décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCRéD)

6

ANNEXES

II. Sur le principe de la licéité des traitements effectués dans le cadre des procédures de la vérification des antécédents ou de « contrôle d'honorabilité »

A titre de remarque liminaire, il y a lieu de relever que les données collectées, dans le cadre des enquêtes administratives, sont initialement collectées et traitées par la Police grand-ducale⁶⁰, par le Ministère public⁶¹ ou par le Service de renseignement de l'Etat (ci-après le « SRE »)⁶² 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. Ces traitements initiaux sont soumis à la loi du 1^{er} 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.

Toutefois, il convient de relever que les traitements de données à caractère personnel mis en œuvre dans le cadre des procédures de la vérification des antécédents ou de « contrôle d'honorabilité » seront soumis au RGPD alors que la finalité poursuivie est le recrutement d'un candidat à un des postes visés par le texte sous avis, ou la délivrance d'une autorisation, d'un permis ou agrément, tels que visés par le projet de loi.

Ainsi, bien que les finalités des traitements envisagés dans le cadre de la loi en projet, soient à des fins administratives, la nature même des données transmises et ensuite utilisées

pour diligenter l'enquête administrative reste identiques à la nature des données traitées 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. Dans un tel contexte, il y a lieu de s'interroger sur l'articulation des dispositions du RGPD avec celles de la loi du 1^{er} 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 problématique est d'ailleurs illustrée à l'article 11, paragraphe (6), de la loi modifiée du 20 avril 1977 sur les jeux de hasard et les paris sportifs, tel que modifié par l'article 5 du projet de loi. Ces dispositions font, en effet, expressément référence à la loi du 1^{er} 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.

1. Sur l'article 6 paragraphe (3) du RGPD

Il y a lieu de féliciter les auteurs du projet de loi sur le fait que, d'un point de vue de la sécurité juridique, le projet de loi instaure une base légale pour les enquêtes effectuées dans le cadre de la vérification des antécédents ou de « contrôle d'honorabilité », conformément à l'article 6, paragraphe (3), du RGPD.

En effet, le traitement de données à caractère personnel collectées et traitées dans le cadre

⁶⁰ V. articles 9 et 14 du projet de loi.

⁶¹ V. articles 4, 6, 7, 11, 12 et 15 du projet de loi.

⁶² V. articles 9 et 14 du projet de loi.

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)⁶³, qui dispose que « [l]e fondement du traitement visé au paragraphe 1, points c) et e), est défini par :

c. le droit de l'Union; ou

d. 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. »

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 énonce encore que « [l]orsque 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

⁶³ 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; (...) ».

6

ANNEXES

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. ».

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.

Bien que la base légale, instaurant les différentes procédures de vérification des antécédents ou de « contrôle d'honorabilité », précise les types de données traitées, les personnes concernées ainsi que les entités auxquelles les données peuvent être communiquées et pour quelles finalités, la Commission nationale relève que certains éléments relatifs au traitement de données ne sont pas suffisamment précisés ou ne sont pas précisés du tout (par exemple la durée de conservation des données) dans le projet de loi.

En outre, les entités qui diligentent les enquêtes, telles que prévues par le projet de loi, seront-elles amenées à tenir un registre qui regroupera l'ensemble des données issues de telles enquêtes ? Le ministre de la Justice ou le ministre des Finances tiendront-ils un registre

dans lequel figureraient les données issues des enquêtes administratives ? Qu'en est-il du Ministère public, tiendra-t-il lui aussi un registre spécifique « enquêtes administratives » ou est-ce que le traitement de données y relatif fera, le cas échéant, partie de la banque de données « JU-CHA » ?

Si tel devait être le cas, la Commission nationale estime essentiel que la création de tels registres soit prévue par le présent projet de loi. Les dispositions légales portant création desdits registres devront contenir les éléments cités ci-dessus. Sur ce point, il est par ailleurs renvoyé aux dispositions légales françaises qui encadrent les registres de données issues des enquêtes administratives⁶⁴. Si de tels fichiers devaient exister, il est recommandé aux auteurs du projet de loi de s'inspirer du système français.

2. Sur les principes dégagés par la jurisprudence de la Cour européenne des droits de l'Homme et de la Cour de justice de l'Union européenne

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

⁶⁴ V. articles R.236-1 à R.236-10 du CSI relatifs au traitement de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique ».

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 (A) ;
- soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité (B) ;
- 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.

Il y a plus précisément lieu d'examiner si les deux premières conditions sont remplies en l'espèce.

A. Sur 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'homme⁶⁵, 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 les droits protégés par la Convention⁶⁶. La législation interne doit être « accessible aux personnes concernées et prévisible quant à ses répercussions »⁶⁷. 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 »⁶⁸ ainsi que « [l]e degré de précision requis de la "loi" à cet égard dépendra du sujet en question. »⁶⁹.

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. Cet encadrement légal serait par ailleurs un garant du principe de sécurité juridique au profit des personnes concernées, des candidats aux postes visés par le texte en projet, ou des demandeurs d'une

⁶⁵ L'article 8 paragraphe (2) de la Convention européenne des droits de l'homme dispose que : « Il ne peut y avoir d'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 ».

⁶⁶ CouEDH, *Fernández Martínez c. Espagne* [GC], n°56030/07, para. 117.

⁶⁷ CouEDH, *Amann c. Suisse* [GC], n° 27798/95, 16 février 2000, para. 50 ; V. 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.

⁶⁸ CouEDH, *Amann c. Suisse* [GC], n° 27798/95, 16 février 2000, para. 56 ; V. 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.

⁶⁹ CouEDH, *The Sunday Times c. Royaume-Uni*, n° 6538/74, 26 avril 1979, para. 49 ; V. également 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.

6

ANNEXES

autorisation, permis ou agrément prévus par le projet de loi sous avis. La sécurité juridique constitue 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 conséquence⁷⁰.

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* »⁷¹. 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* »⁷². 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 »⁷³.

Dès lors, dans la mesure où les traitements de données mis en œuvre dans le cadre des enquêtes administratives, visées par le projet de loi sous avis, constituent une ingérence dans le droit au respect de la vie privée des candidats ou demandeurs d'une autorisation, d'un permis ou agrément, tels que visés par le projet de loi sous avis, celui-ci devrait encadrer plus spécifiquement de tels traitements conformément à la jurisprudence de la Cour européenne des droits de l'Homme. Or, force est de constater que le projet de loi sous avis, tel qu'amendé n'est, par endroit, pas rédigé avec suffisamment de précision⁷⁴. La CNPD reviendra plus particulièrement sur ce point dans ses développements sous les points IV. et V. ci-après.

B. Sur la seconde condition

Il ressort de la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'Homme que les motifs invoqués par les autorités publiques pour justifier une limitation à l'exercice du droit

⁷⁰ V. p.ex. Cour EDH, *Aurubis Balgarie* du 31 mars 2011, C-546/09, points 42-43 ; Arrêt, *Alfamicro c. Commission* du 14 novembre 2017, T-831/14, points 155-157.

⁷¹ Cour EDH, *Amann c. Suisse* [GC], n°27798/95 para 56.

⁷² *Ibidem*. V. 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:CHR:2014:0612JUD005603007, 12 juin 2014 para.117 ; Cour EDH, *Liberty et autres c. Royaume-Uni*, no 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.

⁷³ Arrêt du 8 avril 2014, *Digital Rights Ireland e.a.* C-293/12 et C-594/12, EU:C:2014:238, point 54.

⁷⁴ 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.

à la protection des données à caractère personnel ou une ingérence dans le droit au respect de la vie privée doivent être pertinents et suffisants⁷⁵ et qu'il doit être démontré qu'il n'existe pas d'autres méthodes moins intrusives⁷⁶. La notion de nécessité, telle qu'interprétée par la Cour de justice de l'Union européenne, implique que les mesures adoptées soient moins intrusives que d'autres options pour atteindre le même but. De plus, selon la jurisprudence de la Cour européenne des droits de l'Homme, pour répondre au critère de nécessité, l'ingérence devra également être proportionnée. Dans son « Manuel de droit européen en matière de protection des données », l'Agence des droits fondamentaux de l'Union européenne précise que « [l]a proportionnalité requiert qu'une mesure d'ingérence dans l'exercice des droits protégés par la Cour européenne des droits de l'Homme n'aille pas au-delà de ce qui est nécessaire pour atteindre le but légitime poursuivi. Les facteurs importants à prendre en compte lors de l'appréciation du critère de proportionnalité sont la portée de l'ingérence, notamment le nombre de personnes concernées, et les garanties ou les avertissements mis en place pour limiter sa portée ou ses effets négatifs sur les droits des individus »⁷⁷.

Le Contrôleur européen de la protection des données indique encore qu'« [u]n examen de la proportionnalité suppose en règle générale de déterminer quelles « garanties » doivent accompagner une mesure (qui porterait par

exemple sur la surveillance) afin de réduire à un niveau « acceptable »/proportionné les risques posés par la mesure envisagée au regard des droits fondamentaux et des libertés des individus concernés. »⁷⁸.

En l'occurrence, à défaut de telles précisions dans le projet de loi, quelles seraient les garanties envisagées par les auteurs du projet de loi sous avis ? N'existerait-il pas de méthodes moins intrusives que le système prévu par le texte en projet ?

En ce qui concerne plus particulièrement les enquêtes administratives qui ne porteraient pas uniquement sur la communication d'un extrait de casier judiciaire, il y a lieu de s'interroger sur les conséquences qu'un tel mécanisme est susceptible d'engendrer pour les personnes concernées.

La duplication des informations concernant les antécédents judiciaires d'une personne concernée dans les mains de différentes autorités pourrait être l'une d'entre elles. En effet, la CNPD se demande si à l'issue des enquêtes administratives diligentées par le ministre de la Justice ou le ministre des Finances, des données contenues dans les fichiers tenus par la Police grand-ducale, par le Ministère public ou le SRE seraient amenées à figurer une nouvelle fois dans un fichier tenu par le ministre de la Justice ou le ministre des Finances. Afin d'éviter une duplication de telles données et la tenue d'une sorte de nouveau « casier bis » par le ministre de la Justice ou le

⁷⁵ V. l'arrêt de la Cour européenne des droits de l'homme du 4 décembre 2008, S. et Marper c. Royaume-Uni.

⁷⁶ V. les arrêts de la Cour de justice du 9 novembre 2010, C-92/09, Volker und Markus Schecke GbR/Land Hessen, et C-93/09, Eifert/Land Hessen et Bundesanstalt für Landwirtschaft und Ernährung.

⁷⁷ V. page 45 du « Manuel de droit européen en matière de protection des données » de l'Agence des droits fondamentaux de l'Union européenne.

⁷⁸ V. page 11 des « Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel ».

6

ANNEXES

ministre des Finances, une méthode moins intrusive pour atteindre le même but devrait être préférée au système actuellement prévu par le projet de loi.

Ainsi, il y a lieu d'attirer l'attention des auteurs du projet de loi sur la proposition faite par le Conseil d'Etat, dans son avis complémentaire du 19 décembre 2020 relatif au projet de loi N°7425 sur les armes et munitions⁷⁹, concernant la vérification d'honorabilité visée à l'article 14 du projet de loi précité.

A la place de la procédure de vérification d'honorabilité instaurée par ledit projet de loi, le Conseil d'Etat propose le mécanisme d'un « *avis circonstancié du procureur d'Etat se référant tant aux antécédents judiciaires qu'à l'ensemble des procès-verbaux et rapports pertinents auxquels le procureur d'Etat peut avoir accès, et encore à des informations qui lui sont transmises par la Police grand-ducale* ».

Ce système permettrait d'éviter une duplication des données concernant les antécédents judiciaires de la personne concernée tout en permettant au ministre de la Justice ou au ministre des Finances d'obtenir les informations nécessaires et pertinentes, sous forme d'un avis du Ministère public, afin de lui permettre d'apprécier leur « *honorabilité* ». Un tel mécanisme présenterait encore l'avantage que l'enquête administrative serait confiée à une autorité répressive, le Ministère public, et non pas à une/des administration(s). En effet, une telle autorité serait plus appropriée pour mener

une telle enquête eu égard à la nature des données traitées.

Par ailleurs, il y a lieu de relever que ce mécanisme d'avis du Ministère public est d'ores et déjà prévu pour certaines des procédures de vérification des antécédents visées par le texte en projet⁸⁰. La Commission nationale estime qu'il serait préférable de transposer ce système à l'ensemble des procédures de vérification des antécédents prévues par le projet de loi.

III. Sur l'origine des données

1. L'article 8, paragraphe (1), de la loi du 1^{er} 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 Commission nationale comprend que les données collectées et traitées par le ministre de la Justice, le ministre des Finances ou encore le procureur d'Etat général dans le cadre des procédures de vérification des antécédents ou de « *contrôle d'honorabilité* », proviennent de fichiers tenus par la Police grand-ducale⁸¹, le Ministère public⁸² et le SRE⁸³.

Il y a lieu de constater que ces données ont été initialement collectées par les autorités précitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution

⁷⁹ V. avis complémentaire du Conseil d'Etat du 19 décembre 2020, document parlementaire n°7425/08, développements sous « Amendement 14 ».

⁸⁰ V. articles 4, 6, 7, 11, 12 et 15 du projet de loi.

⁸¹ Articles 9 et 14 du projet de loi.

⁸² Articles 1, 2-3°, 3, 4, 5, 6, 7, 11, 13 et 15.

⁸³ Articles 9 et 14 du projet de loi.

de sanctions pénales et seront dans le cadre du projet de loi traitées pour des finalités ultérieures différentes.

La CNPD se félicite qu'une telle base légale soit prévue par le dispositif sous avis conformément aux dispositions de l'article 8, paragraphe (1), de la loi du 1^{er} 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.

Cet article dispose que « *[l]es données à caractère personnel collectées par les autorités compétentes pour les finalités énoncées à l'article 1^{er} ne peuvent être traitées à des fins autres que celles y énoncées, à moins qu'un tel traitement ne soit autorisé par le droit de l'Union européenne ou par une disposition du droit luxembourgeois.* ».

Néanmoins, il y a lieu de relever que la base légale, sous avis, semble instaurer un régime spécial par rapport aux dispositions du Chapitre 2, section 2, de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière, et à celles prévues par l'article 9 paragraphe (2) de la loi modifiée du 5 juillet 2016 portant réorganisation du SRE.

En effet, ces dispositions ont respectivement pour objet d'encadrer la transmission de telles données par la Police grand-ducale à d'autres administrations dans le cadre de la vérification de l'honorabilité, et la communication par le SRE « *[d]es renseignements collectés dans le cadre*

de ses missions (...) aux administrations dans la mesure où ces renseignements paraissent utiles à l'accomplissement de leurs missions respectives. »⁸⁵.

Il convient de saluer le fait que le projet de loi prévoit expressément :

- la communication des données par le Ministère public au ministre de la Justice ou au ministre des Finances dans le cadre des procédures de vérification des antécédents ou de « contrôle d'honorabilité » alors qu'à ce jour aucune disposition légale ne prévoyait une telle communication ; et
- le traitement de telles données par le Ministère public à des fins d'enquêtes administratives, telles que prévues par le dispositif sous avis.

Enfin, et afin de permettre aux personnes concernées de comprendre l'étendue et la portée de l'enquête administrative, ne serait-il pas préférable d'indiquer dans le projet de loi que les données collectées lors des enquêtes administratives proviennent de fichiers tenus par la Police grand-ducale, le Ministère public ou le SRE ? Sur ce point les auteurs du projet de loi pourraient s'inspirer de la législation française⁸⁶.

Quant aux fichiers tenus par la Police grand-ducale, il convient de relever que le projet de loi n°7741 portant modification 1^o de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, 2^o de la loi modifiée du 5 juillet 2016 portant réorganisation du SRE et 3^o du Code pénal, a été déposé le 30 décembre 2020. Ledit projet

⁸⁴ V. document parlementaire n°6975 sur le projet de loi relative à l'échange de données à caractère personnel et d'informations en matière policière, commentaires des auteurs du projet de loi concernant les articles 26 et suivants du projet de loi.

⁸⁵ V. Article 9 paragraphe (2) de la loi modifiée du 5 juillet 2016 portant réorganisation du SRE.

⁸⁶ V. nos développements sous le point I.3 du présent avis.

6

ANNEXES

de loi a notamment pour objet d'encadrer les traitements des données à caractère personnel effectués dans les fichiers de la Police grand-ducale, et plus précisément dans le fichier central.

Une attention particulière devrait être portée sur l'accès à la partie passive du fichier central. Son accès est, en effet, strictement limité aux finalités énumérées au paragraphe (19) de l'article 43-2 du projet de loi n°7741 (les enquêtes administratives n'y sont pas visées) et est soumis à l'accord du procureur général d'Etat. Dès lors, les auteurs du projet de loi devraient s'assurer de la bonne cohérence et articulation entre les deux textes en projet.

2. La base de données dite « JU-CHA »

Il y a lieu de relever que la base de données dite « JU-CHA » est encadrée actuellement par la seule 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.

Dans son avis du 31 juillet 2020 sur l'application « JU-CHA », l'autorité de contrôle judiciaire précise qu'« [i]l ne fait aucun doute que les traitements de données effectués par les autorités compétentes en matière pénale ainsi qu'en matière de sécurité nationale constituent une ingérence dans le droit au respect de la vie privée et le droit à la protection des données et que les dispositions pénales, en particulier le Code pénal et le Code de procédure pénale, constituent une base légale suffisante pour

la collecte de données à caractère personnel dans l'exécution des missions essentielles du ministère public et des juridictions judiciaires ».

Selon l'autorité de contrôle judiciaire l'application « JU-CHA » constituerait un traitement de données distinct en « *allant au-delà des traitements de données basés sur les procédures pénales* » car celle-ci faciliterait « *l'exploitation et la mise en relation d'informations sur base de procédures judiciaires distinctes* » et permettrait « *des rapprochements entre ces différents traitements de données ayant des finalités connexes* ». Les conditions et les modalités de ce traitement de données ne sont pas prévues par la loi.

Conformément aux développements sous le point II. du présent avis, de telles précisions devraient être prévues par la loi afin de conférer une plus grande sécurité juridique aux justiciables. Le Conseil d'Etat a d'ailleurs justement relevé, dans son avis complémentaire précité relatif au projet de loi n°7425, que la problématique du « contrôle de l'honorabilité » « *renvoie à celle de la base légale des bases de données dites « Jucha »*. Si la tenue de ces fichiers devait recevoir une base légale, on pourrait envisager un système dans lequel le procureur d'Etat est invité à émettre un avis sur la dangerosité du demandeur, y compris au regard d'informations tirées de procès-verbaux et rapports dont il est saisi »⁸⁷.

Ainsi, dans l'hypothèse où le ministre de la Justice entendrait légiférer sur ce point, et compte tenu de l'interaction entre l'application

⁸⁷ V. avis complémentaire du Conseil d'Etat du 19 décembre 2020, document parlementaire n°7425/08, développements sous « Amendement 14 ».

« JU-CHA » et les dispositions sous avis, les auteurs du projet de loi devront veiller à ce que le texte s'articule avec le projet sous avis.

IV. Sur le traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûretés connexes

Aux fins de vérifier l'honorabilité, le projet de loi prévoit que les traitements effectués porteront sur les données à caractère personnel relatives aux condamnations pénales et aux infractions et plus précisément sur les données relatives au casier judiciaire (2) et sur les faits susceptibles de constituer un crime ou un délit ou relatifs à une condamnation pénale pour crime ou délit (3). Or, il convient de rappeler que ces données ne peuvent être traitées que dans le respect des conditions visées à l'article 10 du RGPD (1).

1. Sur le respect des dispositions de l'article 10 du RGPD

L'article 10 du RGPD dispose que « *[l]e traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées.* ». Ledit article précise encore que « *[t]out registre*

complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique ».

A défaut de précision dans le texte sous avis ou par les auteurs du projet de loi dans le commentaire des articles, la Commission nationale se demande quelle seraient les garanties qui seraient prévues ?

Eu égard à la nature des données qui seraient collectées ainsi qu'au niveau de risque lié à la perte de confidentialité de telles données et de leur impact potentiel sur les personnes concernées, il est essentiel que de telles garanties soient prévues dans le projet de loi.

De telles garanties devraient être plus particulièrement prévues pour les procédures de vérification des antécédents de type 2 et 3 alors que celles-ci ne se basent pas uniquement sur l'extrait de casier judiciaire et sont les plus intrusives d'un point de vue de la vie privée des personnes concernées. En effet, celles-ci verront leurs données, relatives à des condamnations pénales ou à des faits susceptibles de constituer des infractions pénales, être consultées ou communiquées au ministre de la Justice, ou au ministre des Finances pour des finalités étrangères à celles pour lesquelles ces données ont été collectées initialement⁸⁸.

Or, il conviendrait d'éviter une duplication de telles données dans les mains de plusieurs autorités⁸⁹, ou d'éviter une multiplicité des accès à de telles données, alors que cela fait

⁸⁸ Il est renvoyé à nos observations formulées au point II. et III. du présent avis.

⁸⁹ Ces derniers disposeraient, le cas échéant, à l'issue des procédures de vérification des antécédents de la copie de rapports de police, extraits de procès-verbaux, jugements, extraits de casier judiciaire, ou encore pour certains cas des « *informations nécessaires* » fournies par le SRE.

6

ANNEXES

courir un risque accru d'accès illégitime à de telles données.

Dès lors, comme indiqué précédemment, il serait préférable de mettre en œuvre un système de vérification des antécédents ou de « contrôle d'honorabilité » se basant sur un avis circonstancié du procureur d'Etat, tel que cela ressort des articles 4, 7, 11, 12 et 15 du projet de loi.

La CNPD estime donc essentiel que des garanties soient prévues par les auteurs du projet de loi. La transmission d'un avis circonstancié du Ministère public à la place des transmissions actuellement prévues par le projet de loi, tel que suggéré par le Conseil d'Etat dans son avis complémentaire du 19 décembre 2020 relatif au projet de loi N°7425 sur les armes et munitions⁹⁰, pourrait être l'une d'entre elles.

2. Sur le traitement de données relatives au casier judiciaire

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. Cette loi porte création de plusieurs bulletins avec une ventilation des inscriptions se trouvant sur les bulletins respectifs.

S'il apparaît que le traitement d'un extrait de casier judiciaire national ou étranger est

un dénominateur commun à l'ensemble des procédures de vérification des antécédents prévues par le projet de loi, des nuances sont, cependant, à distinguer entre les procédures de vérification des antécédents de type 1 (A), de type 2 (B) et de type 3 (C).

A. Sur les procédures de vérification des antécédents de type 1

a. Sur la communication du bulletin N°2 du casier judiciaire

Aux fins de la nomination d'expert, traducteur et d'interprète assermentés, en matière répressive et administrative⁹¹, ou de délivrance d'agrément de médiateur⁹², ou d'agrément de facilitateur de justice restaurative⁹³, le ministre de la Justice sollicitera, pour chacune de ces procédures, que le requérant fournisse un bulletin N°2 de son casier judiciaire.

En effet, le projet de loi précise que le ministre de la Justice « conformément à l'article 8 paragraphe 1^{er}, de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire peut prendre connaissance des inscriptions au bulletin numéro 2 du casier judiciaire du requérant pour vérifier que les antécédents judiciaires de ce dernier ne sont pas incompatibles avec l'exercice des fonctions » des experts, traducteurs, interprètes, médiateur ou facilitateur de justice restaurative.

Cependant, il y a lieu de s'interroger sur la pertinence du renvoi à l'article 8 paragraphe (1) de la loi modifiée du 29 mars 2013 relative à l'orga-

⁹⁰ V. document parlementaire n°7425/08, développements sous « Amendement 14 ».

⁹¹ V. article 3 du projet de loi relatif à l'article 1^{er} de la loi modifiée du 7 juillet 1971 portant en matière répressive et administrative, institution d'experts, de traducteurs et d'interprètes assermentés.

⁹² V. article 2-3° du projet de loi relatif à l'article 1251-3 du Nouveau Code de procédure civile et article 13 du projet de loi relatif à l'article 2 de la loi du 6 mai 1999 relative à la médiation pénale.

⁹³ V. article 1 du projet de loi relatif à l'article 8-1 du Code de procédure pénale.

nisation du casier judiciaire⁹⁴. Cet article renvoie également au règlement grand-ducal 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 »).

En effet, si la volonté des auteurs du projet de loi est de permettre au ministre de la Justice d'obtenir la communication du bulletin N°2 par le Ministère public alors cela devrait être reflété clairement dans le projet de loi. En outre, de telles précisions constitueraient une base légale suffisante afin de permettre au ministre de la Justice d'obtenir le bulletin N°2 du requérant. Dans un tel cas, l'accord du requérant apparaîtrait superfétatoire alors que la communication d'un tel bulletin disposerait, alors, d'une base légale.

En tout état de cause, si les auteurs du projet de loi devaient maintenir de telles dispositions, celles-ci s'avèreraient superfétatoires en ce qui concerne l'article 1 du projet de loi au regard des dispositions du règlement grand-ducal du 23 juillet 2016⁹⁵.

b. Sur la communication d'un extrait de casier judiciaire étranger

Le projet de loi dispose que « *si le requérant est ressortissant d'un autre Etat membre de l'Union*

européenne ou d'un Etat tiers, le ministre de la Justice peut lui demander la remise d'un extrait du casier judiciaire ou d'un document similaire délivré par l'autorité publique compétente du ou des pays dont il a la nationalité ».

Il est encore précisé que sous condition de l'accord du requérant, le « *ministre peut également adresser une demande motivée au procureur général d'Etat en vue de l'obtention d'un extrait du casier judiciaire de l'autorité compétente de l'Etat membre dont le requérant a la nationalité* ».

La Commission nationale se félicite que de telles dispositions soient prévues et comprend que celles-ci s'appliqueraient conformément aux dispositions légales européennes⁹⁶ ou internationales en vigueur en la matière.

Il est renvoyé aux observations formulées au point a., ci-avant, en ce qui concerne la problématique d'une double base légale quant à la communication d'un extrait de casier judiciaire.

B. Sur les procédures de vérification des antécédents de type 2

Il y a lieu de relever que le procureur d'Etat général peut prendre connaissance⁹⁷ ou communiquer le « casier judiciaire » au ministre de la Justice⁹⁸ dans le cadre des procédures aux fins de recrutement visées par :

⁹⁴ L'article 8, paragraphe (1) de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire dispose que « [l]e bulletin N° 2 d'une personne physique ou morale est délivré sur demande : 1) aux administrations de l'Etat, administrations communales et personnes morales de droit public saisies, dans le cadre de leurs missions légales, d'une demande présentée par la personne physique ou morale concernée, laquelle a donné son accord de manière écrite ou électronique afin que le bulletin N° 2 soit délivré directement à l'administration ou à la personne morale de droit public. La liste des administrations et personnes morales de droit public et les motifs d'une demande de délivrance sont fixés par règlement grand-ducal ».

⁹⁵ L'article 1^{er} point 7) du règlement grand-ducal du 23 juillet 2016 dispose que : « [l]e bulletin N° 2 peut être délivré sur demande et avec l'accord exprès de façon écrite ou électronique de la personne concernée : (...) au ministre ayant la Justice dans ses attributions pour l'instruction des demandes relatives aux experts, traducteurs et interprètes assermentés (...) ».

⁹⁶ V. le système informatisé d'échange d'informations sur les casiers judiciaires (le « système ECRIS »).

⁹⁷ V. articles 4, 6, 7, 11 et 15 du projet de loi.

⁹⁸ V. article 5 du projet de loi.

6

ANNEXES

- l'article 16 de la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat⁹⁹ ;
- l'article 11 paragraphe (3) de la loi modifiée du 20 avril 1977 sur les jeux de hasard et les paris sportifs¹⁰⁰ ;
- les articles 76 et 77 de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire¹⁰¹ ;
- l'article 90 bis de la loi modifiée du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif¹⁰² ;
- les articles 2 et 3 de la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice¹⁰³ ; et
- l'article 2 de la loi modifiée du 7 juin 2012 sur les attachés de justice¹⁰⁴.

Ces articles prévoient que le procureur général d'Etat peut prendre connaissance du « casier judiciaire » ou que le ministre de la Justice peut demander au Ministère public la communication du « casier judiciaire » et si « le requérant est ressortissant d'un Etat membre de l'Union européenne ou d'un Etat tiers, le Ministère public peut lui demander la remise d'un extrait de casier judiciaire ou d'un document similaire délivré par l'autorité publique compétente du ou des pays dont il a la nationalité ».

La Commission nationale se félicite que de telles précisions soient apportées par les auteurs du projet de loi.

Cependant, quant à la délivrance d'un extrait de casier judiciaire luxembourgeois, il y a lieu de regretter que le numéro de bulletin du casier judiciaire ne soit pas précisé par le texte en projet.

Afin de respecter le principe de prévisibilité et de précision auquel doit répondre tout texte légal ou réglementaire¹⁰⁵, il est essentiel que les auteurs du projet de loi précisent le numéro de bulletin du casier judiciaire qui serait visé par les dispositions précitées.

En ce qui concerne l'article 11, paragraphe (3), de la loi modifiée du 20 avril 1977 sur les jeux de hasard et les paris sportifs, tel que modifié par le projet de loi, la Commission nationale déduit des dispositions de l'article 1^{er} point 7) du règlement grand-ducal du 23 juillet 2016¹⁰⁶ qu'il s'agirait du bulletin N°2. Si tel devait être le cas, alors cela devrait être expressément indiqué dans le dispositif sous avis.

Quant à la délivrance d'extrait de casier judiciaire pour les ressortissants d'un autre Etat membre de l'Union européenne ou d'un Etat tiers, la CNPD comprend que c'est le demandeur qui fournira directement ledit document.

Contrairement à la procédure de vérification des antécédents type 1, les dispositions relatives à la procédure de vérification des antécédents

⁹⁹ Article 4 du projet de loi.

¹⁰⁰ Article 5 du projet de loi (en ce qui concerne l'autorisation d'exercer un emploi en relation avec des jeux de hasard).

¹⁰¹ Article 6 du projet de loi.

¹⁰² Article 7 du projet de loi.

¹⁰³ Article 11 du projet de loi.

¹⁰⁴ Article 15 du projet de loi.

¹⁰⁵ En ce sens, V. 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; V. entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015.

¹⁰⁶ L'article 1^{er} point 7) du règlement grand-ducal du 23 juillet 2016 dispose que « le bulletin N°2 peut être délivré sur demande et avec l'accord exprès de façon écrite ou électronique de la personne concernée au ministre ayant la Justice dans ses attributions pour l'instruction des demandes relatives aux jeux de hasard ».

type 2 ne précisent pas que, le cas échéant, le ministre de la Justice peut « adresser une demande motivée au procureur général d'Etat en vue de l'obtention d'un extrait du casier judiciaire de l'autorité compétente de l'Etat membre dont le requérant a la nationalité ».

Il y a dès lors lieu de s'interroger sur les raisons de telles différences et si une uniformisation de l'ensemble des trois procédures sur ce point ne serait pas opportune.

C. Sur les procédures de vérification des antécédents de type 3

Ces procédures visent les procédures de vérification des antécédents ou de « contrôle d'honorabilité » relatives aux agréments des services d'adoption¹⁰⁷, aux autorisations d'exploiter des jeux de hasard¹⁰⁸, aux autorisations relatives aux activités privées de gardiennage et de surveillance¹⁰⁹, et aux autorisations, permis ou agréments prévus par la loi modifiée du 15 mars 1983 sur les armes et munitions¹¹⁰.

a. Sur la communication du bulletin N°1 du casier judiciaire

En ce qui concerne les demandes relatives aux agréments des services d'adoption, le projet de loi prévoit que le bulletin N°1, tel que visé par la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire, pourra être consulté, le cas échéant, par le procureur d'Etat.

Or, le bulletin N°1 du casier judiciaire renseigne le relevé intégral des inscriptions applicables à

la même personne et ne peut être délivré qu'aux autorités énumérées à l'article 6 de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire. Ce bulletin est, par exemple, délivré aux autorités judiciaires dans le cadre d'une procédure pénale.

Les auteurs du projet de loi justifient un telle communication compte tenu de « l'obligation de l'Etat de garantir en toutes circonstances le bien-être et les droits de l'enfant, la procédure de vérification des antécédents judiciaires est destinée à renseigner le ministre de la Justice sur le sérieux, l'intégrité et l'aptitude comportementale des responsables du service d'adoption, demandeur d'un agrément. L'avis du procureur d'Etat doit ainsi permettre une appréciation fondée sur des éléments objectifs et aussi complets que possible à travers la consultation du bulletin numéro 1 du casier judiciaire, renseignant toutes les infractions de la personne requérante »¹¹¹.

Sans préjuger le bienfondé d'une telle communication, une telle dérogation devrait néanmoins être justifiée plus amplement par les auteurs du projet de loi. Il est, en effet, difficile d'apprécier si une telle communication respecterait le principe de minimisation des données en l'absence de précision des critères sur lesquels se baseraient le ministre de la Justice pour délivrer ou refuser un tel agrément.

b. Sur la communication du bulletin N°2 du casier judiciaire

En qui concerne les autorisations d'exploiter

¹⁰⁷ Article 12 du projet de loi.

¹⁰⁸ Article 5 du projet de loi (en ce qui concerne l'autorisation d'exploiter des jeux de hasard).

¹⁰⁹ Article 14 du projet de loi.

¹¹⁰ Article 9 du projet de loi.

¹¹¹ V. « Ad article 12 » du projet de loi.

6

ANNEXES

des jeux de hasard¹¹², le projet de loi sous avis prévoit que, pour obtenir l'autorisation d'exploiter des jeux de hasard, le Ministère public « *peut également prendre connaissance des inscriptions du casier judiciaire* » afin de vérifier que le « *comportement de la personne requérante, agissant comme représentant d'une personne morale ou à titre individuel n'est pas incompatible avec l'exploitation de jeux de hasard* »¹¹³.

Le dispositif sous avis ne précise cependant pas le numéro de bulletin du casier judiciaire qui serait consulté. Néanmoins, la Commission nationale déduit des dispositions de l'article 1, point 7) du règlement grand-ducal du 23 juillet 2016¹¹⁴ que le bulletin n°2 du casier judiciaire serait collecté aux fins de délivrance des autorisations relatives aux jeux de hasard.

Si tel devait être le cas, alors cela devrait être reflété dans le dispositif sous avis afin de respecter le principe de prévisibilité et de précision auquel doit répondre tout texte légal ou réglementaire¹¹⁵.

En ce qui concerne les autorisations relatives aux activités privées de gardiennage et de surveillance¹¹⁶, et aux autorisations, permis

ou agréments prévus par la loi modifiée du 15 mars 1983 sur les armes et munitions¹¹⁷, les textes sous avis, qui sont rédigés à l'identique, ne visent pas expressément la communication du bulletin N°2 du casier judiciaire. En effet, les dispositions sous avis disposent que « *le procureur général d'Etat communique au Ministre copie des décisions judiciaires qui figurent le cas échéant sur le bulletin N°2 du casier judiciaire* ».

S'il ressort du projet de loi n°7425 sur les armes et munitions, notamment de l'article 15 paragraphe (4) dudit projet de loi, que le bulletin N°2 serait collecté, cela n'est pas prévu par la loi modifiée du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance.

Cependant, la Commission nationale déduit des dispositions de l'article 1, point 7) du règlement grand-ducal du 23 juillet 2016¹¹⁸ que le bulletin n°2 du casier judiciaire serait collecté pour les autorisations relatives aux activités privées de gardiennage et de surveillance.

Dès lors, afin de respecter le principe de prévisibilité et de précision auquel doit répondre tout texte légal ou réglementaire¹¹⁹,

¹¹² V. article 5 du projet de loi relatif à l'article 11 paragraphe (2) de la loi modifiée du 20 avril 1997 sur les jeux de hasard et les paris sportifs.

¹¹³ V. article 11 paragraphe (1) de la loi modifiée du 20 avril 1997 sur les jeux de hasard et les paris sportifs, tel que modifié par l'article 5 du projet de loi.

¹¹⁴ L'article 1^{er}, point 7) du règlement grand-ducal du 23 juillet 2016 dispose que « *le bulletin N°2 peut être délivré sur demande et avec l'accord exprès de façon écrite ou électronique de la personne concernée au ministre ayant la Justice dans ses attributions pour l'instruction des demandes relatives aux jeux de hasard* ».

¹¹⁵ En ce sens, V. 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; V. entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015.

¹¹⁶ V. article 14 du projet de loi.

¹¹⁷ V. article 9 du projet de loi.

¹¹⁸ L'article 1^{er}, point 7) du règlement grand-ducal du 23 juillet 2016 dispose que « *le bulletin N°2 peut être délivré sur demande et avec l'accord exprès de façon écrite ou électronique de la personne concernée au ministre ayant la Justice dans ses attributions pour l'instruction des demandes en matière d'armes prohibées et de gardiennage* ».

¹¹⁹ En ce sens, V. 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; V. entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015.

des précisions à ce sujet mériteraient d'être apportées par les auteurs du projet de loi en ce qui concerne les autorisations relatives aux activités privées de gardiennage et de surveillance.

c. Sur la communication d'un extrait de casier judiciaire étranger

En ce qui concerne la communication d'un extrait de casier judiciaire étranger, il y a lieu de relever que les procédures relatives aux agréments de services d'adoption ou aux autorisations d'exploiter des jeux de hasard prévoit qu'« *en cas de besoin le procureur d'Etat peut demander l'obtention du casier judiciaire de l'autorité compétente de l'Etat membre* » dont la personne concernée a la nationalité.

Il y a lieu de s'interroger sur l'utilisation de la formulation « en cas de besoin » alors que ce terme est vague et ne permet pas de comprendre quelles seraient les situations où la communication d'un extrait de casier judiciaire s'avèrerait nécessaire ou non.

Dès lors, afin de respecter le principe de prévisibilité et de précision auquel doit répondre tout texte légal ou réglementaire¹²⁰, la CNPD estime que des précisions sur ce point soient apportées. De plus, dans un souci de cohérence du projet de loi dans son ensemble, celles-ci devraient être rédigées de manière similaire à celles visées par les procédures visées sous les points IV.2. points A. et B. du présent avis.

Par ailleurs, il y a lieu de relever qu'une autre formulation est utilisée pour les procédures de vérification des antécédents relatives aux fins de délivrance d'autorisations relatives aux activités privées de gardiennage et de surveillance¹²¹, et d'autorisations, permis ou agréments prévus par la loi modifiée du 15 mars 1983 sur les armes et munitions¹²².

En effet, les articles 9 et 14 du projet de loi précisent que les condamnations prononcées à l'étranger ou par une juridiction pénale d'un autre Etat membre de l'Union européenne, d'un pays associé à l'espace Schengen ou de l'Espace économique européen sont à prendre en compte lors de la vérification de l'honorabilité. Sur ce point, il est renvoyé aux observations formulées par la CNPD dans son avis complémentaire du 4 février 2021 sur le projet de loi N°7425 sur les armes et munitions¹²³.

Par ailleurs, la Commission nationale s'interroge sur les raisons pour lesquelles des formulations différentes sont employées par les auteurs du projet de loi en ce qui concerne la communication d'un extrait de casier judiciaire étranger. Les disparités entre chacune desdites dispositions sont source d'illisibilité et d'insécurité juridique pour les personnes concernées.

3. Sur le traitement de données relatives à des faits susceptibles de constituer un crime ou un délit, ou relatifs à une condamnation pénale pour crime ou délit

¹²⁰ *ibidem*

¹²¹ V. article 14 du projet de loi.

¹²² V. article 9 du projet de loi.

¹²³ V. avis complémentaire de la CNPD du 04/02/2021, délibération n°2/2021, les développements formulés sous le point I.1.F.c.

6

ANNEXES

Outre la prise de connaissance d'un extrait de casier judiciaire, il y a lieu de relever que les procédures de vérification des antécédents de type 2 et 3 sont plus intrusives que celles de type 1, basées uniquement sur la communication d'un extrait de casier judiciaire. En effet, les procédures de type 2 et 3 se basent également sur les faits :

- susceptibles de constituer un crime ou un délit qui font l'objet d'un procès-verbal ou d'un rapport de police (B) ;
- relatifs à une condamnation pénale pour crime ou délit (C).

Sans préjuger de l'appréciation *in concreto* qui serait effectuée en la matière, il y a lieu de regretter que ni le projet de loi sous avis, ni les commentaires des articles ne précisent quels critères ou quel degré de gravité des antécédents sont pris en compte par le ministre de la Justice, le ministre des Finances ou le Ministère public pour apprécier l'honorabilité des personnes concernées.

Si les auteurs du projet de loi justifient de telles intrusions alors que ces éléments sont notamment destinés à « vérifier que le comportement du candidat n'est pas incompatible avec l'exercice des fonctions et missions de notaire » ou qu'« [i]l est important que les juges et les parquetiers puissent (...) procéder à la vérification des antécédents du personnel dans le cadre de leur recrutement, eu égard à la sensibilité des informations portées à la connaissance du personnel de l'administration judiciaire et de l'honnêteté

requis pour les traiter avec la confidentialité de mise » ou parce qu'« [e]n tant qu'officiers publics il doit être garanti que les huissiers de justice exercent leur fonction avec l'intégrité nécessaire. Cette appréciation doit se faire en tenant compte des antécédents judiciaires » ou encore que la vérification des antécédents judiciaires est « destinée à renseigner le ministre de la Justice sur le sérieux, l'intégrité et l'aptitude comportementale des responsables du service d'adoption. ». Celles-ci ne sont pas formulées avec suffisamment de précisions.

Or, en l'absence de telles précisions, il est difficile d'apprécier si le principe de minimisation des données serait respecté. Il y a lieu de rappeler qu'en vertu de ce principe, seules peuvent être traitées les données à caractère personnel qui sont strictement nécessaires à la réalisation des finalités poursuivies.

A. Remarques liminaires

Il y a lieu de relever que les articles 4, 5, 6, 7, 9, 11, 12, 14 et 15 du projet de loi précisent que la vérification des antécédents portera sur des faits susceptibles de constituer un crime ou un délit.

Seuls les articles 9, 12 et 14 du projet de loi précisent qu'outre les faits susceptibles de constituer un crime ou un délit, la vérification portera sur les faits « visés à l'article 563, point 3° du Code pénal relatif aux voies de fait et de violences légères », « visés à l'article 1^{er} de la loi modifiée du 8 septembre 2003 sur la violence domestique ».

Il est encore intéressant de noter que les auteurs du projet de loi précisent dans leur commentaire de l'article 5 relatif aux autorisations d'exploitation des jeux de hasard et d'exercer un emploi en relation avec des jeux de hasard, que seules certaines infractions semblent particulièrement pertinentes pour refuser de telles autorisations, notamment « lorsqu'il s'agit d'une infraction pénale en lien avec le blanchiment d'argent, le vol, les cas de fraude, etc. ».

Dès lors, ne serait-il pas possible, à l'instar des articles 9, 12 et 14 du projet de loi, d'indiquer avec plus de précision sur quels crimes ou délits portent de telles vérifications ?

B. Sur les faits susceptibles de constituer un crime ou un délit qui font l'objet d'un procès-verbal ou d'un rapport de police

Il y a lieu de relever que les procédures de vérification des antécédents de type 2¹²⁴ ne portent que sur les faits susceptibles de constituer un crime ou un délit qui font l'objet d'un procès-verbal ou d'un rapport de police, si ces faits font l'objet d'une poursuite pénale en cours, à l'exclusion des faits ayant abouti à une décision de non-lieu ou de classement sans suites.

La Commission nationale se demande si, a contrario, en l'absence de précision sur ce point, les procédures de vérification des antécédents de type 3¹²⁵ incluent les faits ayant abouti à une décision de non-lieu ou de

classement sans suites. Cela mériterait d'être clarifié par les auteurs du projet de loi.

En ce qui concerne le traitement de données relatives à de tels faits, il y a particulièrement lieu d'attirer l'attention des auteurs du projet de loi sur le fait qu'« un procès-verbal ou un rapport ne sont pas l'équivalent d'une décision de justice ayant retenu une personne dans les liens de la prévention et que le principe de la présomption d'innocence doit prévaloir. »¹²⁶.

En ce qui concerne les faits qui font l'objet d'une poursuite pénale en cours, les auteurs du projet de loi devraient porter une attention particulière au secret de l'instruction. A ce titre, il y a lieu de relever que seuls les articles 5, 9 et 14 du projet de loi précisent que lorsque les faits sont couverts par le secret de l'instruction seules les données énumérées par ces articles peuvent être communiquées.

Il y a lieu de constater que pareilles précisions ne sont pas apportées par les articles 4, 6, 7, 11, 12 et 15 du projet de loi. Or, bien qu'il s'agisse de procédures lors desquelles une enquête administrative soit diligentée par le procureur d'Etat général et qu'un avis de ce dernier soit émis à l'issue de celles-ci, ne faudrait-il pas prévoir des dispositions spécifiques visant à restreindre le contenu d'un tel avis lorsque des faits sont couverts par le secret de l'instruction ?

En l'absence des raisons justifiant de telles différences entre les articles précités sur ce point, la CNPD est d'avis qu'une uniformisation des dispositions à ce sujet serait opportune.

¹²⁴ V. les procédures visées aux articles 4, 5 (volet autorisation d'exercer un emploi), 6, 7, 11 et 15 du projet de loi.

¹²⁵ V. les procédures visées aux articles 5, 9, 12 et 14 du projet de loi.

¹²⁶ V. avis complémentaire du Conseil d'Etat du 19 décembre 2020 relatif au projet de loi N°7425 sur les armes et munitions, document parlementaire n°7425/08, développements sous « Amendement 14 ».

En outre, et comme relevé par le Conseil d'Etat dans son avis complémentaire relatif au projet de loi N°7425 sur les armes et munitions¹²⁷, quelle serait la portée du secret de l'instruction par rapport aux règles de la procédure administrative non contentieuse et contentieuse ?

C. Sur les faits relatifs à une condamnation pénale pour crime ou délit

Il y a lieu de relever que les procédures de vérifications de type 2 excluent les faits relatifs à une condamnation pénale pour crime ou délit pour laquelle la réhabilitation a été atteinte (a) contrairement à la procédure de type 3 qui, en l'absence de précision, ne semble pas l'exclure (b).

Par ailleurs, à titre de remarque générale, il y a lieu de s'interroger sur l'apport de la communication de données relatives à des faits concernant une condamnation pénale pour crime ou délit alors que le projet de loi prévoit d'ores et déjà la communication d'un extrait de casier judiciaire, voir pour certains des articles du projet de loi la communication de la décision figurant, le cas échéant, au casier judiciaire¹²⁸. En effet, est-il pertinent de communiquer des décisions qui ne seraient pas encore définitives ou non encore inscrites au casier judiciaire de la personne concernée ?

a. Sur les procédures de vérification des antécédents de type 2

Les procédures visées par les articles repris sous le petit a) excluent les faits relatifs à une

condamnation pénale pour crime ou délit et pour laquelle la réhabilitation n'est pas déjà atteinte au moment de l'introduction de la demande de candidature.

Malgré ces précisions, le projet de loi n'indique pas les raisons pour lesquelles les données relatives à une condamnation pénale pour crime ou délit sont nécessaires et pertinentes afin de vérifier l'honorabilité de la personne concernée. Ces précisions sont essentielles alors que la communication d'un extrait de casier judiciaire permet d'ores et déjà de renseigner sur les condamnations prononcées à l'encontre d'un requérant.

Afin de respecter le principe de prévisibilité et de précision auquel doit répondre tout texte légal ou réglementaire¹²⁹, il est essentiel que les auteurs du projet de loi précisent les catégories de données qui seraient visées par les dispositions précitées.

S'agit-il seulement de décisions judiciaires ou de tous documents se rapportant à une condamnation pénale pour crime ou délit ?

b. Sur les procédures de vérification des antécédents de type 3

Contrairement aux procédures visées sous le petit a) précité, les procédures visées par les articles 5, 9, 12 et 14 ne précisent pas si les faits relatifs à une condamnation pénale, pour laquelle la réhabilitation aurait été atteinte, sont exclus par lesdites procédures. Seule une limitation dans le temps pour ces faits est

¹²⁷ V. avis complémentaire du Conseil d'Etat du 19 décembre 2020 relatif au projet de loi N°7425 sur les armes et munitions, document parlementaire n°7425/08, développements sous « Amendement 14 ».

¹²⁸ V. articles 9 et 14 du projet de loi.

¹²⁹ En ce sens, V. 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; V. entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015.

précisée par lesdits articles. En effet, les articles disposent tous que « *[I]es faits ne peuvent avoir été commis plus de cinq ans avant l'introduction de la demande du requérant, sauf si ces faits ont fait l'objet d'une condamnation pénale, auquel cas le délai de cinq ans est porté à dix ans, ou lorsque ces faits font l'objet d'une procédure pénale en cours* ».

Des justifications devraient être apportées par les auteurs du projet de loi quant aux raisons pour lesquelles les données relatives à une condamnation pénale pour crime ou délit sont nécessaires et pertinentes afin de vérifier l'honorabilité de la personne concernée.

En outre, il y a lieu de constater que les articles 9 et 14 du projet de loi prévoient que sur demande « *le procureur d'Etat communique au Ministre copie des décisions judiciaires qui figurent le cas échéant sur le bulletin N°2 du casier judiciaire de la personne concernée* ». Sur ce point, il est renvoyé aux développements de la Commission nationale dans son avis complémentaire relatif au projet de loi n°7425¹³⁰.

Dès lors, et afin de respecter le principe de prévisibilité et de précision auquel doit répondre tout texte légal ou réglementaire¹³¹, il est essentiel que les auteurs du projet de loi précisent les catégories de données qui seraient visées par les dispositions précitées.

Par ailleurs, la CNPD se demande si de telles dispositions sont nécessaires en ce qui concerne l'ensemble des autorisations visées par les articles 5 et 8 de la loi du 12 novembre 2002

relative aux activités privées de gardiennage et de surveillance ? Ces dispositions ne seraient-elles pas nécessaires uniquement pour les cas où le personnel engagé serait amené à solliciter un permis de port d'armes ? En outre, cela n'est-il pas d'ores et déjà prévu par l'article 11 de la loi du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance ? Les auteurs du projet de loi relèvent d'ailleurs que « *les mêmes conditions que ceux de la loi sur les armes et munitions s'appliquent donc pour le port d'armes en matière de gardiennage* »¹³².

V. Sur le traitement de catégories particulières de données à caractère personnel

Il ressort des articles 9 et 14 du projet de loi que des catégories particulières de données au sens de l'article 9 du RGPD seraient amenées à être traitées par le ministre de la Justice.

En effet, des données relatives à la santé des requérants et plus précisément à leur « santé mentale » seraient amenées à être collectées par le ministre de la justice dans le cadre de la vérification de leur honorabilité. En ce qui concerne la collecte de telles données par le ministre de la Justice dans le cadre de l'article 9 du projet de loi, il est renvoyé à la délibération n°42/2019 du 8 juillet 2019 de la CNPD¹³³.

La CNPD comprend encore que des données qui révèlent les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne sollicitant un

¹³⁰ V. avis complémentaire de la CNPD du 04/02//2021, délibération n°2/2021, point I. F. a. ii., page 16

¹³¹ En ce sens, V. 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; V. entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015

¹³² V. commentaires des auteurs du projet de loi « *Ad article 14* ».

¹³³ Avis de la CNPD sur le projet de loi n°7425 sur les armes et munitions, délibération n°xx, v. les observations formulées sous le point IV. « Sur le traitement de données relatives aux infractions pénales et à la santé » page 10.

6

ANNEXES

agrément, permis ou autorisation, tels que visés par les articles précités, seraient susceptibles d'être échangées entre le ministre de la Justice et le SRE. Les auteurs du projet de loi précisent, à ce sujet, que l'échange de données entre le SRE et le ministre de la Justice a été introduit compte tenu du « *contexte politique actuel au niveau des tendances extrémistes violentes* », contexte qui « *démontre l'importance pour les autorités de pouvoir vérifier plus en détail la personne qui soumet une autorisation d'acquérir, d'acheter, d'importer, d'exporter, de transférer, de transporter, de détenir, de porter, de vendre et de céder des armes et munitions* ».

Par ailleurs, dans le cadre du contrôle de l'honorabilité, tel que visé aux articles 4, 5, 6, 7, 11, 12 et 15 du projet de loi, il n'est pas exclu que d'autres catégories particulières de données, telles que des données relatives à l'origine raciale ou ethnique, des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, pourront être traitées.

Or, il y a lieu de rappeler que conformément à l'article 9 paragraphe (1) du RGPD « *[l]e traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des don-*

nées concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits », sauf si l'une des conditions visées au paragraphe (2) dudit article s'applique.

La Commission nationale est d'avis que le traitement de catégories particulières de données, lors des enquêtes administratives qui seraient diligentées par le ministre de la Justice, le ministre des Finances ou le Ministère public, pourrait se baser sur l'article 9 paragraphe (2), lettre g) du RGPD, à condition de toutefois en respecter les conditions.

Cet article dispose que « *[l]e 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* ».

Or, force est de constater que le projet de loi ne semble pas prévoir les « *mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* ». Dès lors, le texte sous projet, ne semble pas offrir un fondement juridique suffisant pour traiter ces catégories de données particulières.

Afin de rendre licite de tels traitements de données, il est donc indispensable que de telles mesures soient définies dans le projet de loi sous avis.

Il conviendrait également de préciser expressément que des catégories particulières de données pourraient être collectées alors que cela ne résulte pas expressément de la lecture des articles 4, 5, 6, 7, 9, 11, 12, 14 et 15 du projet de loi. Ainsi, il est suggéré que les auteurs du projet de loi s'inspirent de la législation française, en matière d'armes, et plus précisément de l'article R.312-85 point VI du CSI intitulé « données et informations issues de l'enquête administrative ». Sur ce point, il est renvoyé à l'avis complémentaire de la Commission nationale sur les amendements du projet de loi N°7425 sur les armes et munitions¹³⁴.

Par ailleurs, il y a lieu de s'interroger sur la nécessité de tels traitements de données en ce qui concerne l'ensemble des autorisations visées par les articles 5 et 8 de la loi du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance ? Ces dispositions ne seraient-elles pas nécessaires uniquement pour les cas où le personnel serait amené à solliciter un permis de port d'armes ?

Or, à ce titre, il ressort, d'ores et déjà, de l'article 16, paragraphe (2), nouveau du projet de loi n°7425 que « [s]i le permis de port d'armes est demandé pour un agent de gardiennage au sens de la loi modifiée du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance, l'attestation médicale peut être délivrée par un des médecins visés aux points 1° et 2°, ou par le médecin du travail compétent, après avis favorable d'un des médecins visés aux points 1° et 2°. ».

Les auteurs du projet de loi devraient veiller dès lors, à la bonne articulation entre les dispositions sous avis et les dispositions de l'article 16, paragraphe (2), nouveau du projet de loi n°7425 sur les armes et munitions.

VI. Sur les modalités de transmission des données issues des procédures de vérification des antécédents judiciaires ou de « contrôle d'honorabilité »

Il y a lieu de relever que les modalités de transmission des données issues des procédures de vérification des antécédents ne sont pas suffisamment précisées ou ne sont pas précisées du tout par le projet de loi. Il convient encore de relever le manque d'uniformisation entre les différentes dispositions sous avis sur ce point.

Ainsi, il ressort des procédures de vérification des antécédents visées aux articles 4, 7, 11, 12 et 15 du projet de loi, que les données issues de l'enquête administrative seraient transmises via l'avis du procureur général d'Etat. Ces avis sont transmis aux autorités compétentes pour la nomination d'un notaire¹³⁵ ou d'un huissier de justice¹³⁶, le recrutement du personnel de l'administration judiciaire¹³⁷, des juridictions de l'ordre administratif¹³⁸ et des attachés de justice¹³⁹ ou la délivrance d'un agrément en matière des services d'adoption¹⁴⁰. Il y a lieu de relever que seules des données pertinentes et nécessaires devraient être transmises via cet avis afin

¹³⁴ Avis de la CNPD sur le projet de loi n°7425 sur les armes et munitions, délibération n°2/2021 du 04/02/2021, v. les observations formulées sous le point IV. « Sur le traitement de données relatives aux infractions pénales et à la santé » page 10.

¹³⁵ Article 4 du projet de loi.

¹³⁶ Article 11 du projet de loi.

¹³⁷ Article 6 du projet de loi.

¹³⁸ Article 7 du projet de loi.

¹³⁹ Article 15 du projet de loi.

¹⁴⁰ Article 12 du projet de loi.

6

ANNEXES

de permettre aux autorités compétentes d'apprécier l'honorabilité des candidats ou requérants.

Pour les procédures visées aux articles 9 et 14 du projet de loi, les données seraient communiquées par la Police grand-ducale, le Ministère public ou le SRE au ministre de la Justice « *sous forme de l'intégralité ou d'extraits de procès-verbaux ou rapports de police, jugements, arrêts, ordonnances, ou tout autre document ou acte de procédure contenant les informations concernées* ». Sur ce point, il est renvoyé aux observations formulées par la Commission nationale dans son avis complémentaire sur les amendements du projet de loi N°7425 sur les armes et munitions¹⁴¹.

Aucune précision ne sont cependant apportées en ce qui concerne les modalités de transmission des données collectées lors des enquêtes visées aux articles 5 et 6 du projet de loi.

La CNPD estime essentiel que des précisions sur ces points soient apportées par les auteurs du projet de loi et rappelle que seul les données nécessaires et pertinentes ne peuvent être communiquées.

En tout état de cause, comme évoqué tout au long du présent avis, il serait préférable que les auteurs du projet de loi optent pour un système qui se baserait sur la communication d'un avis circonstancié du procureur d'Etat général.

VII. Sur la mise en place d'un système de suivi en ce qui concerne la vérification de l'honorabilité

La CNPD comprend qu'un système de suivi quant à la condition de l'honorabilité serait mis en place, tel que cela ressort des articles 3, 9 et 14 du projet de loi.

En ce qui concerne les articles 9 et 14 du projet de loi dans la mesure où ceux-ci sont rédigés à l'identique, la Commission nationale renvoie sur ce point à ses observations formulées dans son avis complémentaire sur les amendements du projet de loi N°7425 sur les armes et munitions¹⁴².

L'article 3 du projet de loi relatif à la désignation, en matière répressive et administrative, des experts, traducteurs et des interprètes assermentés, prévoit que le ministre de la Justice « *pourra révoquer* » les experts, traducteurs ou interprètes assermentés « *en cas de manquement à leurs obligations ou à l'éthique professionnelle ou pour d'autres motifs graves. La révocation ne pourra intervenir que sur avis du procureur général d'Etat et après que l'intéressé aura été admis à présenter ses explications* ».

Les auteurs du projet de loi ne précisent pas le fonctionnement d'un tel système. Il y a, dès lors, lieu de s'interroger sur le système de suivi qui serait le cas échéant mis en place. Le procureur général d'Etat consultera-t-il la base de données dite « JU-CHA » de façon proactive et régulière afin de faire remonter,

¹⁴¹ V. avis complémentaire de la CNPD sur les amendements du projet de loi N°7425, délibération n°2/2021 du 04/02/2021, v. les observations formulées sous le point IV. « Sur le traitement de données relatives aux infractions pénales et à la santé » page 10.

¹⁴² Avis complémentaire de la CNPD sur le projet de loi n°7425 sur les armes et munitions, délibération n°2/2021 du 04/02/2021, v. les observations formulées sous le point I.2., page 19.

en cas d'incident, au ministre de la Justice des informations susceptibles d'entraîner la révocation des personnes concernées ?

Par ailleurs, il convient de noter que de telles dispositions ne sont pas prévues pour les autres procédures de vérification des antécédents, si tel devait être le cas alors cela devrait être reflété dans le projet de loi sous avis.

VIII. Sur le principe d'exactitude des données

Conformément à l'article 5, paragraphe (1), lettre d) du RGPD, les données à caractère personnel doivent être « *exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder* ».

Or, il y a lieu de constater que le dispositif sous avis ne prévoit aucune disposition relative à la mise à jour des données obtenues dans le cadre des enquêtes administratives. Or, compte tenu des données collectées, il convient d'attirer l'attention des auteurs du projet de loi sur le fait qu'il existe un risque important que des données relatives à une personne dont l'affaire a été classée sans suite ou qui a entretemps été acquittée d'une infraction dont elle a été accusée se trouvent toujours dans les dossiers de l'administration, sans une mise à jour ou rectification afférente.

IX. Sur le principe de limitation des finalités

Conformément au principe de 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.

En ce qui concerne les procédures qui ne seraient pas diligentées par le Ministère public, il y a lieu de relever que la transmission des données provenant de fichiers tenus par la Police grand-ducale, le Ministère public ou encore le SRE vers le ministre de la Justice ou le ministre des Finances à des fins d'enquête administrative est très délicate voire risquée et doit, dès lors, être limitée à des situations exceptionnelles et strictement limitées.

Ainsi, l'utilisation des données à des fins autres que celles pour lesquelles elles ont été transmises aux ministres, comporte des risques additionnels et semble a priori difficilement justifiable. Une telle utilisation ultérieure devrait en tout état de cause respecter les conditions de l'article 6, paragraphe (4), du RGPD et faire l'objet d'une loi « *du moins quant aux éléments essentiels de la matière* » conformément à l'article 11, paragraphe (3), de la Constitution¹⁴³.

Par conséquent, à l'instar des dispositions prévues à l'article 26, paragraphes (2) et (3), de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informa-

¹⁴³ V. en ce sens, M. Besch, « Traitement de données à caractère personnel dans le secteur public », Normes et légistique en droit public luxembourgeois, Luxembourg, Promoculture Larcier, 2019, p.471 à 472, n°619.

6

ANNEXES

tions en matière policière¹⁴⁴, ne faudrait-il pas prévoir dans le projet de loi sous avis que les données qui seraient transmises au ministre de la Justice ou au ministre des Finances à des fins d'enquête administrative ne peuvent être utilisées que pour la finalité pour laquelle elles ont été transmises et encadrer la transmission, le cas échéant, par le ministre à une autre administration/ à un tiers ? Ne faudrait-il pas également le prévoir pour les avis qui seraient transmis par le Ministère public aux autorités visées par les articles 4, 7, 11, 12 et 15 du projet de loi ?

X. Sur la durée de conservation

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. Au-delà, les données doivent être supprimées ou anonymisées.

Il y a lieu de relever que les auteurs du projet de loi ont, à plusieurs reprises, indiqué que « *[C]es données ne seront conservées que pendant la durée strictement nécessaire à l'octroi ou au refus définitif de l'agrément demandé* »¹⁴⁵ ou « *au refus définitif de l'autorisation ou de l'agrément demandé* »¹⁴⁶ ou encore « *pendant la durée strictement nécessaire à l'examen de la candidature* »¹⁴⁷. Il y a lieu de relever que ces

précisions ne sont pas reprises pour chacun des articles visés par le projet de loi.

Néanmoins, ces précisions ne permettent pas à la Commission nationale d'apprécier si, en l'occurrence, le principe de durée de conservation limitée des données serait respecté.

Or, il est essentiel que des précisions à ce sujet soient apportées et ce d'autant plus eu égard à la nature des données à caractère personnel en cause. Ainsi, la durée de conservation devrait être définie dans le projet de loi ou 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 lors des enquêtes administratives.

Par ailleurs et afin de tenir compte d'éventuels recours à l'encontre des décisions administratives qui seraient prises en vertu du projet de loi, il est suggéré aux auteurs du projet de loi de s'inspirer de la législation française en matière d'armes, qui fixe une durée de conservation pour les données issues de l'enquête administrative. L'article R.312-88 du CSI dispose que : « *[I]es données à caractère personnel et informations mentionnées au d du 1^o du I et aux V et VI de l'article R.312-85 [les données issues de l'enquête administrative] sont*

¹⁴⁴ L'article 26 paragraphes (2) et (3) dispose que : « (2) Les données et informations transmises ne peuvent être utilisées par l'administration que pour la finalité pour laquelle elles ont été transmises. Elles sont effacées dès que leur conservation n'est plus nécessaire au regard de la finalité pour laquelle elles ont été transmises. (3) La transmission ultérieure des données et informations par l'administration de l'État à une tierce personne requiert l'accord préalable écrit de la personne visée à l'article 18, paragraphe 1^{er}, ayant transmis les données et informations concernées. Le cas échéant, l'article 6, paragraphe 3, est applicable ».

¹⁴⁵ V. paragraphe (5) de l'article 1251-3 du Nouveau Code de procédure civile, tel que modifié par l'article 2-3^o du projet de loi, paragraphe (4) de l'article 1 de la loi modifiée 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, tel que modifié par l'article 3 du projet de loi, paragraphe (4) de l'article 2 de la loi du 6 mai 1999 relative à la médiation pénale, tel que modifié par l'article 13 du projet de loi.

¹⁴⁶ V. paragraphe (6) de l'article 11 de la loi modifiée du 20 avril 1977 sur les jeux de hasard et les paris sportifs, tel que modifié par l'article 5 du projet de loi.

¹⁴⁷ V. article 90 bis de la loi modifiée du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif, tel que modifié par l'article 7 du projet de loi.

conservées pendant une durée maximale d'un an à compter de la notification des décisions mentionnées au IV du même article ou, en cas de recours contentieux dirigé contre ces décisions, jusqu'à ce qu'il ait été définitivement statué sur le litige».

XI. Sur le droit des personnes concernées

Selon l'article 5 paragraphe (1) lettre (a) du RGPD, les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (principe de licéité, loyauté, transparence). Ce principe implique notamment que le ministre de la Justice, le ministre des Finances ou le Ministère public devront respecter les dispositions de l'article 13 du RGPD pour les données collectées directement auprès de la personne concernée, sinon celles de l'article 14 du RGPD, lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée elle-même, c'est-à-dire celles collectées indirectement auprès du Ministère public, de la Police grand-ducale ou du SRE.

En vertu de ces articles, le responsable du traitement devra fournir à la personne concernée des informations au sujet du traitement la concernant, notamment pour garantir un traitement équitable et transparent. Il est précisé que dans les cas où l'article 14 du RGPD s'appliquerait, ces informations devront être fournies à la personne concernée au plus tard un mois après que le responsable du traitement ait obtenu les données.

A toutes fins utiles, il y a lieu de préciser que la législation française en matière d'armes prévoit, à l'article R.312-90 du CSI, une restriction des droits des personnes concernées (voir Chapitre III du RGPD). Cet article dispose notamment que : « *[L]es droits d'information, d'accès, de rectification et à la limitation des données mentionnés aux articles 13 à 16 et 18 du [RGPD] et aux articles 104 à 106 de la loi du 6 janvier 1978 précitée s'exercent auprès du service central des armes ou du préfet territorialement compétent, en fonction de leurs attributions respectives. Afin d'éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires ou d'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 ou de protéger la sécurité publique, les droits d'accès, de rectification et à la limitation peuvent faire l'objet de restrictions en application de l'article 52 et des 2° et 3° du II et du III de l'article 107 de la loi du 6 janvier 1978 précitée.* »

Dès lors, il y a lieu d'attirer l'attention des auteurs du projet de loi sur le fait que sans dérogation explicite dans le projet de loi, ces droits sont tous applicables intégralement. Or, de telles dérogations pourraient s'avérer opportunes lorsque les informations obtenues dans le cadre de certaines procédures de vérification des antécédents concernent des enquêtes ou instructions pénales en cours.

XII. Sur la sécurité du traitement

Conformément à l'article 5 paragraphe (1) lettre f) du RGPD les données à caractère personnel

6

ANNEXES

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)* ».

L'article 32 du RGPD dispose encore 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, des fuites de données ou des modifications non désirées.

La CNPD est d'avis que la protection de la confidentialité et de la sécurité des données à caractère personnel constitue un enjeu majeur en cas de traitement de catégories particulières de données dans la mesure où leur divulgation est susceptible de constituer un préjudice grave pour les personnes concernées.

Ainsi, eu égard à la nature des données traitées en cause, il est essentiel que de telles mesures de sécurité soient mises en œuvre par les différents responsables du traitement afin d'assurer la confidentialité et la sécurité des données.

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. Il est intéressant de noter qu'en France, les articles R.234-1 à R.234-3 et R.236-6 du CSI énumère les catégories de personnes autorisées à accéder aux données qui seraient issues de l'enquête administrative.

Dans ce contexte, il est vivement recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début la personne ou le service, au sein de chaque administration concernée, qui aurait accès à l'interface informatique mise à disposition par le CTIE, et à quelles données précises cette personne ou ce service aurait accès.

En outre, il est nécessaire de prévoir un système de journalisation des accès. Sur ce point, la CNPD recommande que les données de journalisation soient conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.

Enfin, en ce qui concerne les données qui seraient initialement soumises à la loi du 1^{er} 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, se pose la question de l'articulation, le cas échéant, entre les dispositions prévues à l'article 28 de ladite loi et de celles prévues à l'article 32 du RGPD.

XIII. Sur l'autorité de contrôle compétente

Il y a lieu de s'interroger sur le fait de savoir quelle est l'autorité de contrôle compétente pour contrôler et surveiller le respect des dispositions légales prévues par le texte en projet, en l'absence de précision à ce sujet dans le projet de loi sous avis.

En effet, il existe un doute sur le point de savoir si les données, collectées initialement pour les besoins de la prévention, de la recherche, de la constatation et de la poursuite des infractions, puis transmises par la Police grand-ducale, le Ministère public et le SRE au ministre de la Justice ou au ministre des Finances afin de lui permettre de vérifier l'honorabilité d'un candidat, demandeur de permis, autorisation ou agrément visés par le projet de loi relève de la compétence de l'autorité de contrôle judiciaire¹⁴⁸ ou de celle de la Commission nationale.

Il y a lieu de rappeler que le paragraphe (2) de l'article 40 de la loi du 1^{er} 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 dispose que *« 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, que ce soit pour les finalités visées à l'article 1^{er} de la présente loi ou pour celles visées par le [RGPD], sont soumises au contrôle de l'autorité de contrôle judiciaire »*.

Les auteurs du projet de loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale estiment que *« pour déterminer la compétence d'une des deux autorités de contrôle [CNPD ou autorité de contrôle judiciaire], la question déterminante ne sera plus la finalité de la donnée concernée, mais celle de savoir si l'autorité compétente participe à la prise ou à l'exécution d'une décision juridictionnelle, ce qui n'est pas le cas pour la Police »*¹⁴⁹.

Ils précisent encore que *« lorsque pour un traitement de données à caractère personnel déterminée – relevant du champ d'application du présent projet de loi – la question de la compétence d'une des deux autorités de contrôle se pose, il faudrait en principe retenir la compétence de la Commission nationale pour la protection des données, sauf si le traitement de données à caractère personnel concerné est effectué par une juridiction dans l'exercice de ses fonctions juridictionnelles ou par le ministère public, soit dans l'exercice de ses fonctions juridictionnelles, soit en amont ou en aval de sa participation à la prise d'une décision juridictionnelle »*¹⁵⁰.

En l'espèce, le ministre de la Justice et le ministre des Finances ne constituent pas une des autorités visées par l'article 40 de la loi de la loi du 1^{er} 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

¹⁴⁸ Autorité de contrôle de judiciaire telle que visée par l'article 40 de la loi du 1^{er} 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.

¹⁴⁹ V. document parlementaire n°7168, « Ad article 41 », page 47.

¹⁵⁰ V. document parlementaire n°7168, « Ad article 41 », page 47.

6

ANNEXES

nationale, et ne sont pas susceptibles de rendre une décision juridictionnelle à l'issue de l'enquête administrative mais une décision purement administrative.

Dès lors, le traitement de données effectué par ces ministres dans le cadre des enquêtes administratives, visées par le projet de loi, pourrait tomber dans le champ de compétence de la Commission nationale.

Il est intéressant de noter que cette solution a été retenue en ce qui concerne l'autorité compétente pour surveiller et contrôler les dispositions de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière¹⁵¹.

Ne faudrait-il pas retenir la même solution en ce qui concerne les traitements effectués par le Ministère public lorsque celui-ci diligente les enquêtes administratives, tel que cela est prévu par le projet de loi sous avis ?

Dans un souci de lever tout équivoque sur ce point, les auteurs du projet de loi devrait compléter le dispositif sous avis en conséquence.

A toutes fins utiles, il y a lieu de relever que la compétence de la CNPD en ce qui concerne les traitements de données effectués par lesdits ministres dans le cadre du projet de loi sous avis ne préjuge en rien de la compétence de l'autorité de contrôle judiciaire en ce qui concerne la communication de données par le Ministère public à ces ministres, tel que prévu par le projet de loi.

XIV. Sur les autres lois visées par le projet de loi mais étrangères au « contrôle d'honorabilité »

Le projet de loi entend également modifier les articles 1007-6 et 1036 du Nouveau Code de procédure civile ainsi que la loi du 30 décembre 1981 portant indemnisation en cas de détention préventive inopérante et 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. Il y a lieu de relever que ces dispositions ne portent pas sur le contrôle de l'honorabilité.

En ce qui concerne les dispositions sous avis portant modification des articles 1007-6 et 1036 du Nouveau Code de procédure civile, il y a lieu de relever que ces dispositions relèvent des missions exercées par le Ministère public en matière civile.

Lesdits articles prévoient encore que le procureur d'Etat pourra, dans le cadre de ces procédures « *prendre connaissance des inscriptions au bulletin N°1 du casier judiciaire* » ainsi que, le cas échéant, du « *casier judiciaire de l'autorité compétente de l'Etat dont les parties à l'audience ont la nationalité* ». Il y a lieu de féliciter les auteurs du projet de loi pour de telles précisions.

La CNPD comprend encore que les auteurs du projet de loi entendent prévoir un accès par le Ministère public à la base de données dite « JU-CHA » dans le cadre des procédures

¹⁵¹ Articles 25, paragraphe (1), et 28 de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière.

visées aux articles 1007-6 et 1036 du Nouveau Code de procédure civile.

Sans préjuger du bienfondé d'un tel accès, la CNPD se demande toutefois, s'il ne serait pas plus pertinent de prévoir de telles dispositions dans un texte de loi relatif à la base de données « JU-CHA » et à son utilisation par le Ministère public dans le cadre de l'exercice de ses missions ?

En ce qui concerne l'article 2 de la loi du 30 décembre 1981 portant indemnisation en cas de détention préventive inopérante, tel que modifié par le projet de loi, il y a lieu de saluer les précisions apportées en ce qui concerne les données qui seraient traitées dans le cadre de l'instruction de la demande en réparation telle que prévue par la loi précitée.

Enfin, en ce qui concerne l'article 9 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, tel que modifié par le projet de loi, il y a lieu de féliciter les auteurs du projet de loi de prévoir une base légale en ce qui concerne l'échange de données entre le ministre de la Justice, le Ministère public et l'administration de l'Enregistrement.

XV. Remarques finales

Il y a lieu de relever que les dispositions du projet de loi sous avis qui reprennent l'article 5 du RGPD¹⁵² sont susceptibles d'être super-

fétatoires. En effet, le RGPD est, en tant que règlement européen, obligatoire dans tous ses éléments et directement applicable au Luxembourg. La Commission nationale se permet d'attirer l'attention des auteurs du 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'Etat rappelle régulièrement dans ses avis la jurisprudence de la Cour de justice de l'Union européenne selon laquelle les Etats membres ne doivent pas entraver l'applicabilité directe des règlements ni en dissimuler la nature européenne¹⁵³.

Ainsi décidé à Belvaux en date du 10 février 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

¹⁵² V. articles 1, 3, 5, 6, 7, 13 et 15 du projet de loi.

¹⁵³ V. par. ex. l'avis du Conseil d'Etat 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.

6

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7768 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19. (Délibération n°5/AV4/2021 du 16/02/2021)

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 12 février 2021, Madame la Ministre de la Santé a saisi la Commission nationale d'une demande d'avis sur le projet de loi n°7768 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 (ci-après le « projet de loi n°7768 »).

Il ressort de l'exposé des motifs que le présent projet de loi vise à maintenir les restrictions

actuellement en place tout en prévoyant un certain nombre de précisions concernant, entre autres, le « *régime applicable en matière de traitement des données à caractère personnel, notamment pour ce qui est du programme de dépistage à grande échelle et dans le cadre de la vaccination.* »

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.

I. Ad article 4 du projet de loi n°7768

L'article 4 du projet de loi n°7768 vise à modifier diverses dispositions 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 (ci-après : « loi modifiée du 17 juillet 2020 »). La CNPD formule trois remarques à cet égard :

1. A l'article 5 paragraphe (1) de la loi modifiée du 17 juillet 2020 est ajoutée une nouvelle catégorie de personnes pouvant accéder aux données relatives à la santé dans le cadre de l'activité du traçage des contacts et qui doivent être nommément désignées par le directeur de la santé. En effet, le paragraphe en cause dispose dorénavant que les personnes infectées doivent renseigner 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 « *le directeur de la santé ou son délégué, ainsi que les fonctionnaires, employés ou les salariés mis à disposition du ministère de la Santé en application de l'article L. 132-1 du Code du travail ou toute autre personne, désignés à cet effet par le directeur de la santé* ».

Le commentaire des articles précise que « *cet ajout vise uniquement à pouvoir s'adapter à l'évolution de la situation épidémiologique, notamment au regard des différents variants existants, et permettre d'ajuster les capacités de l'équipe en charge du suivi et du traçage par le biais de volontaires appelés en renfort, si nécessaire. Cette nouvelle catégorie vise plus particulièrement le personnel de soins retraité.* »

La CNPD estime par contre que le libellé actuel du projet de loi n°7768, et plus particulièrement le bout de phrase ajouté à savoir « *toute autre personne* », est plus que vague et elle estime qu'une telle formulation ne saurait en aucun cas légitimer un éventuel traçage des contacts interne mis en œuvre par des employeurs privés ou publics, en parallèle au traçage mis en œuvre par la Direction de la santé. En effet, eu égard au risque que certains employeurs privés ou publics pourraient procéder, de bonne foi, à un contact tracing interne, elle relève que la licéité d'un tel contact tracing est loin d'être juridiquement claire dans la législation actuelle.

2. Lors du Conseil de gouvernement du 25 janvier 2021, les ministres réunis avaient marqué leur accord avec l'introduction d'une obligation de présenter un test SARS-CoV-2 négatif avant l'embarquement pour toutes les personnes se déplaçant vers le Grand-Duché de Luxembourg par voie aérienne.¹⁵⁴ Ainsi, depuis le 29 janvier 2021, « *toute personne, indépendamment de sa nationalité, âgée de 6 ans ou plus, souhaitant se déplacer par transport aérien à destination du Grand-Duché de Luxembourg, doit présenter à l'embarquement le résultat négatif (sur papier ou document électronique) d'un test de détection virale par PCR de l'ARN viral du SARS-CoV-2 ou d'une recherche de l'antigène viral (test rapide) réalisé moins de 72 heures avant le vol* ».¹⁵⁵

La CNPD se demande dans ce contexte si, en sus du traitement prévu à l'actuel article 5 paragraphe 2bis de la loi modifiée du 17 juillet 2020, c'est-à-dire la collecte de données à caractère personnel par le biais des formulaires de localisation des passagers, un traitement supplémentaire de données à caractère personnel par les compagnies aériennes aurait lieu, comme par exemple la conservation d'une copie du test négatif ou l'enregistrement des données y relatives. Dans cette hypothèse, comme les données à caractère personnel incluses dans un test négatif sont à considérer comme des données concernant la santé¹⁵⁶, les compagnies aériennes procèdent à un traitement

¹⁵⁴ Voir communiqué de presse sur le résumé des travaux du conseil de gouvernement du 25 janvier 2021 : https://gouvernement.lu/fr/actualites/toutes_actualites/communiqués/2021/01-janvier/25-conseil-gouvernement.html.

¹⁵⁵ Voir communiqué du ministère de la Santé et du ministère des Affaires étrangères et européennes du 26 janvier 2021 : <https://covid19.public.lu/fr/actualite-covid-19/communiqués/2021/01/26-mesures-sanitaires-deplacements.html>.

¹⁵⁶ L'article 4 point 15 du RGPD définit les données concernant la santé comme « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.* » Le considérant (35) du RGPD précise que les données à caractère personnel concernant la santé devraient comprendre : « *[...] des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle [...]* ».

6

ANNEXES

portant sur des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD. Le traitement de telles données étant en principe interdit en vertu de l'article 9 paragraphe (1) du RGPD, les compagnies aériennes doivent se baser sur une des dix conditions d'exemption prévues au paragraphe (2) de l'article 9 du RGPD.

La CNPD estime que l'unique condition applicable en l'espèce serait l'article 9 paragraphe 2) lettre i) du RGPD (traitement nécessaire pour des motifs d'intérêts public dans le domaine de la santé publique), lu ensemble avec l'article 6 paragraphe (1) lettre c) du RGPD (traitement nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis). Dans ces 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'Etat 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 Etat 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, au cas où sur base de la décision prise en conseil de gouvernement un traitement de données à caractère personnel est mis en œuvre par les compagnies aériennes au moment où les passagers présentent leur test SARS-CoV-2 négatif avant l'embarquement, la CNPD recommande aux auteurs du projet de loi de prévoir ce traitement soit dans le corps du texte du projet de loi sous avis, soit dans un autre texte légal afin de satisfaire 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.

3. En vertu de l'article 5 paragraphe (3) premier point de la loi modifiée du 17 juillet 2020, les professionnels de santé sont déjà obligés, en vue de suivre et d'acquérir les connaissances fondamentales sur l'évolution de la propagation du virus SARS-CoV-2, de transmettre au directeur de la santé ou à son délégué les nom, prénoms, sexe, numéro d'identification ou date de naissance ainsi que la commune de résidence ou l'adresse des personnes dont le résultat d'un test diagnostique de l'infection au virus SARS-CoV-2 a été négatif. Par contre, ledit point ne prévoit plus que ces données sont anonymisées par le directeur de la santé ou son délégué à l'issue d'une durée de soixante-douze heures après leur réception. Le commentaire de l'article précise que « la référence à la période de conservation qui figure au même point est substituée par la modification proposée à l'article 10, paragraphe 5. »

Ainsi, il résulte d'une lecture combinée des articles 5 paragraphe (3) premier point et 10 paragraphe (5) de la loi modifiée du 17 juillet 2020, tels que modifiés par le projet de loi sous revue, que les données à caractère personnel des personnes dont le résultat d'un test diagnostique de l'infection au virus SARS-CoV-2 a été négatif sont pseudonymisées au plus tard à l'issue d'une durée de six mois après leur collecte pour une période de trois ans à l'issue de laquelle elles sont anonymisées, c'est-à-dire qu'elles sont conservées au total pendant trois ans et demi.

La Commission nationale tient à souligner qu'elle ne dispose pas de l'expertise scientifique et épidémiologique nécessaire afin d'évaluer s'il est justifié et proportionné que les données des personnes dont le résultat d'un test diagnostique de l'infection au virus SARS-CoV-2 a été négatif soient dorénavant conservées pendant trois ans et demi et non plus pendant uniquement 72 heures. En l'absence d'explications plus précises par les auteurs du projet de loi, elle ne peut ainsi pas apprécier si d'éventuelles nouvelles connaissances acquises dernièrement sur le virus du SARS-Cov-2 permettent de justifier pourquoi ces données devraient être conservées pendant un laps de temps beaucoup plus long qu'initialement prévu par le législateur.

II. Ad article 5 du projet de loi n°7768

L'article 5 du projet de loi vise à modifier diverses dispositions de l'article 10 de la loi modifiée du 17

juillet 2020. De nouveau, la CNPD tient à émettre trois observations à cet égard :

1. L'article 10 paragraphe (1bis) nouveau de la loi modifiée du 17 juillet 2020 prévoit que la « *Direction de la santé est responsable des traitements visés au paragraphe 1^{er}, à l'exception de l'identification des catégories de personnes à inviter dans le cadre des programmes de dépistage à grande échelle et de vaccination qui relève de la responsabilité de l'Inspection générale de la sécurité sociale.* » Le commentaire des articles précise que ce « *nouveau paragraphe 1bis est inséré en vue de refléter la responsabilité de l'Inspection générale de la sécurité sociale, partie prenante aux traitements de données effectués dans le cadre des programmes de dépistage à grande échelle et de vaccination, notamment en ce qui concerne la gestion des invitations. Cette dernière dispose de l'expertise et des données démographiques et socio-économiques nécessaires à l'échantillonnage des personnes à inviter dans le cadre du programme de dépistage à grande échelle et du programme de vaccination, en fonction de l'évolution de l'épidémie au Luxembourg.* »

Il en ressort que les auteurs du projet de loi n°7768 considèrent que l'Inspection générale de la sécurité sociale (ci-après : « IGSS ») assume la fonction de responsable du traitement au sens de l'article 4 point 7 du RGPD¹⁵⁷ en ce qui concerne les données à caractère personnel traitées dans le cadre de la gestion des invitations liées au

¹⁵⁷ L'article 4 point 7 du RGPD définit le responsable du traitement comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.* »

6

ANNEXES

programme de dépistage à grande échelle et du programme de vaccination.

La CNPD tient à souligner que pour être qualifié de responsable du traitement, l'IGSS devrait pouvoir décider sur les moyens des traitements susvisés, c'est-à-dire prendre la décision sur base de quels critères quelles personnes seront invitées à se faire tester/vacciner, sans qu'un échange des données à caractère personnel des personnes qui ont reçu une telle invitation avec la Direction de la Santé ne devrait avoir lieu. Par contre, si la Direction de la Santé décide sur base de quels critères les personnes seront invitées à se faire tester/vacciner et que l'IGSS sélectionne uniquement les personnes répondant auxdits critères et envoie pour le compte de la Direction les invitations correspondantes, l'IGSS serait plutôt à considérer comme sous-traitant de la Direction de la Santé.¹⁵⁸

2. En ce qui concerne précisément le rôle de l'IGSS, l'article 10 paragraphe (3bis) nouveau de la loi modifiée du 17 juillet 2020 prévoit que « *l'Inspection générale de la sécurité sociale est destinataire des données traitées qu'elle pseudonymise pour les fins énoncées au paragraphe 6* », c'est-à-dire à des fins de recherche scientifique ou historique ou à des fins statistiques. Le commentaire des articles précise que ce nouveau paragraphe 3bis « *est inséré pour transférer les données à l'Inspection générale de la sécurité sociale afin qu'elle les pseudonymise au travers de son dispositif technique sécurisé et les*

mette à disposition des organismes publics de recherche, conformément à ses missions légales. »

La Commission nationale se demande dans quelle mesure l'IGSS, qui devrait a priori dans ce contexte précis être considéré comme sous-traitant de la Direction de la santé, aurait un accès permanent et continu au système d'information de ladite Direction afin de pseudonymiser régulièrement en bloc toutes les données y contenues ? Ou est-ce que l'IGSS ne recevrait que sur demande, en fonction d'une recherche spécifique et des critères de recherche y liés, des données à caractère personnel contenues dans le système d'information afin de les pseudonymiser ? Dans ce dernier cas, il est primordial que soient mises en œuvre des mesures techniques et organisationnelles appropriées conformément à l'article 32 du RGPD pour sécuriser les flux de communication entre la Direction de la Santé et l'IGSS.

Notons d'ailleurs que la CNPD a déjà à maintes reprises insisté sur la nécessité d'un encadrement législatif de l'activité de tiers de confiance qui permettrait d'accompagner le développement de services innovants en matière de pseudonymisation et d'anonymisation au Luxembourg.¹⁵⁹

3. La CNPD ne peut qu'approuver que dans un but de renforcer la transparence des traitements effectués,¹⁶⁰ le nouveau point 2bis du paragraphe 2 de l'article 10 de la loi

¹⁵⁸ L'article 4 point 8 du RGPD définit le sous-traitant comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.* »

¹⁵⁹ Voir par exemple son avis complémentaire relatif au projet de loi n° 7061 modifiant certaines dispositions du Code de la sécurité sociale, délibération n° 930/2017 du 17 novembre 2017.

¹⁶⁰ Voir commentaire de l'article 5 du projet de loi n°7768.

modifiée du 17 juillet 2020 énumère en détail les données traitées par l'IGSS en vue d'établir la liste des personnes à inviter dans le cadre du programme de dépistage à grand échelle et du programme de vaccination.

Pourtant, au regard du principe de minimisation des données (article 5 paragraphe (1) lettre c) du RGPD), elle s'interroge si le traitement de données sur la composition du ménage, ainsi que sur l'employeur (en sus des données sur le secteur d'activité professionnelle), est vraiment nécessaire en vue de l'identification des catégories de personnes à inviter dans le cadre desdits programmes de dépistage à grand échelle et de vaccination.

De manière générale, la CNPD félicite les auteurs du projet de loi n°7768 sous examen d'avoir déterminé de manière plus précise les finalités des données à caractère personnel collectées dans le cadre du programme de vaccination concernant le vaccinateur et la personne à vacciner, ainsi que les durées de conservation desdites données, qui ont été adaptées en fonction du nombre de données strictement nécessaire au regard des finalités envisagées et du délai de conservation de vingt ans. Le commentaire des articles donne en plus davantage d'explications à cet égard en expliquant par exemple que la « période de vingt ans se justifie au regard de la pharmacovigilance, finalité pour laquelle les dossiers de cas notifiés sont généralement conservés pour une période de vingt ans au moins. L'objectif est de pouvoir revenir au dossier afin d'établir le lien entre les effets secondaires

d'un patient et le vaccin lui administré. A titre d'exemple, la campagne de vaccination déployée dans le cadre de la pandémie H1N1 en 2009 a démontré que les dossiers de pharmacovigilance nécessitaient une conservation longue des données associées. Ainsi, suite à l'identification de la narcolepsie comme effet indésirable avéré du vaccin contre le H1N1, les personnes vaccinées ont pu soumettre des demandes d'indemnisation pour lesquelles il était nécessaire d'associer un patient / un vaccin / un effet afin de pouvoir établir le lien de causalité. Or, deux vaccins avaient été administrés, il fallait donc être en mesure d'identifier lequel fut administré à quel patient. »

Par ailleurs, la CNPD note avec satisfaction que les auteurs du projet de loi n°7768 ont pris en compte le commentaire formulé dans son avis relatif au projet de loi n°7738 modifiant la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid19 sur l'origine des données à caractère personnel des vaccinateurs et des personnes vaccinées¹⁶¹ en ce sens que le paragraphe 2 point 5 de l'article 10 de la loi modifiée du 17 juillet 2020 prévoit dorénavant que ce sont les vaccinateurs ou les personnes placées sous leur responsabilité qui enregistrent sans délai les données visées au point 3° a) et b) du paragraphe en cause concernant précisément le vaccinateur et la personne à vacciner.

Finalement, comme le système d'information mis en place par la Direction de la santé contient

¹⁶¹ Délibération n°30/2020 du 22 décembre 2020.

6

ANNEXES

des données à caractère personnel concernant les personnes vaccinées, par déduction, un fichier sur les personnes non-vaccinées pourrait être créé. Or, la CNPD comprend qu'un tel traitement de données, source potentielle de discrimination et de stigmatisation, ne sera pas mis en œuvre, ni par la Direction de la santé, ni par l'IGSS.

Ainsi décidé à Belvaux en date du 16 février 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 2 décembre 2020, Monsieur le Ministre des Sports a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal relatif à la détermination et à l'organisation des formations des cadres techniques et administratifs pour les différentes formes d'activités sportives (ci-après désigné le « projet de règlement grand-ducal »).

Selon l'exposé des motifs, le sport au Luxembourg englobe l'activité physique dans toutes ses formes, telles que le sport scolaire, le sport-santé, le sport pour personnes handicapées, le sport pour tous, le sport-

**Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal relatif à la détermination et à l'organisation des formations des cadres techniques et administratifs pour les différentes formes d'activités sportives.
(Délibération n°6/AV5/2021 du 24/02/2021)**

fitness, le sport loisir, le sport de compétition et le sport de haut niveau. Afin que l'intégralité de la population puisse exercer ces activités physiques ou sportives d'une manière qui soit adaptée à ses besoins, elle doit être encadrée par des personnes disposant d'une formation adéquate et, partant, des compétences nécessaires à cette fin.

Il ressort encore de l'exposé des motifs que le cadre réglementaire actuel date des années 1990 de sorte qu'il est devenu nécessaire de l'adapter à la réalité contemporaine et d'abroger le règlement grand-ducal du 16 janvier 1990 portant restructuration des cours de formation des entraîneurs dans l'intérêt des fédérations et sociétés sportives ainsi que le règlement grand-ducal du 16 janvier 1990 portant restructuration de la formation des animateurs de sport-loisir.

Par ailleurs, le projet de règlement grand-ducal constitue la suite du programme « *subside qualité+* » introduit par le règlement grand-ducal du 23 décembre 2016 concernant les subsides accordés aux clubs sportifs affiliés auprès d'une fédération sportive agréée et octroyés sur base de la qualification des entraîneurs de jeunes inférieurs à 16 ans.

6

ANNEXES

Dans le présent avis, la Commission nationale abordera les questions liées à la protection des données à caractère personnel soulevées par le titre V, intitulé « Registre électronique », du projet de règlement grand-ducal.

1. Ad article 55 du projet de règlement grand-ducal

L'article 55 du projet de règlement grand-ducal prévoit la création, sous l'autorité du ministre ayant dans ses attributions les Sports, d'un registre électronique, intitulé « registre des brevets », qui a pour finalités « *l'organisation, la gestion et le suivi administratif des formations initiales et continues, visant à l'obtention des différents brevets, brevets d'État, homologations et licences ENEPS y afférentes, ainsi que des dispenses accordées* ». Ainsi, la Commission nationale se félicite que les auteurs du projet de règlement grand-ducal ont pris le soin de déterminer le responsable du traitement ainsi que les finalités de ce registre.

Le commentaire des articles précise que « *[I] a mise en place d'une telle base de données électronique s'inscrit dans les efforts de digitalisation entrepris par les administrations luxembourgeoises* » et vise à faciliter et à optimiser les tâches administratives de l'ENEPS. A cet égard, la Commission nationale tient à rappeler que le RGPD s'applique non seulement aux fichiers informatisés mais également aux fichiers papiers qui, le cas échéant, existent déjà¹⁶².

2. Ad article 56 du projet de règlement grand-ducal

L'article 56, paragraphe 1^{er}, du projet de règlement grand-ducal énonce que le registre des brevets est subdivisé en trois parties, tout en précisant les catégories de données à caractère personnel qui figureront dans les différentes parties.

La CNPD salue le fait que le projet de règlement grand-ducal définit les catégories de données à caractère personnel qui seront renseignées dans le registre des brevets. Elle tient toutefois à rappeler l'importance du principe de minimisation des données consacré à l'article 5, paragraphe 1^{er}, lettre c) du RGPD selon lequel 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. Au vu des explications fournies dans le commentaire des articles, les données à caractère personnel renseignées dans le registre des brevets semblent être limitées à ce qui est nécessaire au regard des finalités énoncées à l'article 55 du projet de règlement grand-ducal.

L'article 56, paragraphe 2, du projet de règlement grand-ducal poursuit que « *[I]es données visées aux points 1^o à 3^o du paragraphe 1^{er} peuvent être communiquées au responsable de traitement de la banque de données en relation avec l'exécution du règlement grand-ducal modifié du 23 décembre 2016 concernant les subsides accordés aux clubs sportifs affiliés auprès d'une fédération sportive agréée* ».

¹⁶² Cf. article 2, paragraphe 1^{er}, du RGPD.

Selon le commentaire des articles, cette communication s'effectue dans l'optique de l'attribution du subside « qualité + » régi par le règlement grand-ducal modifié du 23 décembre 2016. Les auteurs affirment que « *[c]ette communication peut en effet être indispensable, car l'obtention et le montant du subside « qualité + » sont fonction de la qualité de l'encadrement offert aux jeunes par les clubs de sport affiliés* ».

L'utilisation des données du registre des brevets à des fins d'attribution du subside « qualité + » semble être une finalité compatible avec celles décrites à l'article 55 du projet de règlement grand-ducal, d'autant plus que le ministre ayant dans ses attributions les Sports est également le responsable du traitement de la banque de données prévue par le règlement grand-ducal modifié du 23 décembre 2016.

Toutefois, les explications succinctes fournies par les auteurs du projet de règlement grand-ducal ne permettent pas à la Commission nationale d'apprécier s'il y a une réelle nécessité de communiquer les données figurant dans le registre des brevets. En tout état de cause, il semble peu probable qu'il soit nécessaire de communiquer toutes les données figurant dans le registre des brevets, telles que le numéro de téléphone ou l'adresse email. Or, le principe de minimisation des données exige que seules les données effectivement nécessaires à l'attribution du subside « qualité + » soient transmises.

3. Ad article 57 du projet de règlement grand-ducal

L'article 57 du projet de règlement grand-ducal dispose que le ministre ayant dans ses attributions les Sports est le responsable du traitement au sens du RGPD et attribue au directeur de l'ENEPS la qualité de sous-traitant au sens du RGPD.

Cet article poursuit que « *[l]'accès aux fichiers est sécurisé et les informations relatives à la personne ayant procédé à la consultation, aux informations consultées, à la date, à l'heure et la référence du dossier, ainsi qu'au motif précis de la consultation peuvent être retracés.* » Etant donné que cette disposition se trouve au deuxième paragraphe de l'article 57 relatif au sous-traitant, il serait possible d'en déduire qu'elle ne s'applique qu'aux accès effectués par le sous-traitant. Or, la CNPD considère que cette disposition devrait s'appliquer à tous les accès, c'est-à-dire également aux accès effectués par le responsable du traitement lui-même, et propose dès lors de l'insérer dans un paragraphe à part.

Par ailleurs, la Commission nationale note que le projet de règlement grand-ducal ne définit pas la durée de conservation des données à caractère personnel figurant dans le registre des brevets. Le responsable du traitement devra néanmoins veiller à se conformer à l'article 5, paragraphe 1^{er}, lettre e) du RGPD selon lequel les données à caractère personnel conservées sous une forme permettant l'identification des personnes concernées

6

ANNEXES

pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. La Commission nationale estime nécessaire que le projet de règlement grand-ducal précise la/les durée(s) de conservation des données ou des moins les critères applicables pour déterminer les durées de conservation.

Finalement, la CNPD tient à rappeler que les droits des personnes concernées prévus par le RGPD devront être respectés. Ainsi, en vertu des articles 13 et 14 du RGPD, le responsable du traitement est obligé de fournir aux personnes concernées un certain nombre d'informations lorsque des données à caractère personnel sont collectées directement auprès d'elles ou indirectement à travers un tiers, par exemple à travers un club ou une fédération.

Ainsi décidé à Belvaux en date du XX janvier 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 du 6 juillet 2020, le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer au sujet du projet de loi n° 7632 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et portant modification de la loi modifiée du 30 mai 2005 portant: 1) organisation de l'Institut Luxembourgeois de Régulation; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat.

Ladite directive (UE) 2018/1972 est censée remplacer quatre directives actuellement

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7632 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et portant modification de la loi modifiée du 30 mai 2005 portant: 1) organisation de l'Institut Luxembourgeois de Régulation; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat. (Délibération n°7/AV6/2021 du 03/03/2021)

en vigueur. Parmi les directives à remplacer ne figure pas la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive dite vie privée et communications électroniques ou « directive ePrivacy ») transposée au Luxembourg par la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques. Si une proposition de règlement européen devant succéder à ladite directive est en voie d'élaboration, la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques restera en vigueur pour l'instant.

Dans ce contexte, la CNPD tient à faire part de ses observations par rapport à certains articles du projet de loi présentant des aspects ayant trait à la protection des données à caractère personnel, ainsi que concernant les interactions entre le projet de loi sous objet, la loi précitée du 30 mai 2005 et, le cas échéant, le Règlement dit « ePrivacy » en projet¹⁶³.

¹⁶³ Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »).

6

ANNEXES

A la différence de ses textes prédécesseurs, la directive (UE) 2018/1972 et le projet de loi sous avis incluent les fournisseurs de services dits « over the top » ou « OTT » dans leur champ d'application. En effet, sont visés non seulement les services « traditionnels » basés sur la numérotation mais également les services de communications interpersonnelles non fondés sur la numérotation.

Ad article 2

Comme il a été mentionné en introduction du présent avis, la notion de service de communications électroniques est élargie de manière à intégrer les « over the top players » offrant des services de communications interpersonnelles non fondés sur la numérotation.

Cependant, à la différence de ce qui est prévu par le projet de loi sous avis¹⁶⁴, la nouvelle définition du service de communications électroniques devra s'appliquer non seulement à la future loi sur les réseaux et les services de communications électroniques, mais également à la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

En effet, l'article 125 troisième alinéa de la directive (UE) 2018/1972 à transposer dispose ce qui suit : « *Les références faites aux directives abrogées s'entendent comme faites à la présente directive et sont à lire selon le tableau de correspondance figurant à l'annexe XIII.* »

Selon le tableau de l'annexe XIII, toute référence à l'article 2, point c) de la directive 2002/21/

CE (qui définit les services de communications électroniques) s'entendra désormais comme faite à l'article 2, point 4) de la directive (UE) 2018/1972 (repris par l'article 2 paragraphe (4) du projet de loi).

Or, l'article 2 de la directive ePrivacy (2002/58/CE) se réfère justement – sans le mentionner de manière explicite – à l'article 2, point c) de la directive 2002/21/CE par les termes suivants : « *Sauf disposition contraire, les définitions figurant dans la directive 95/46/CE et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive «cadre»)(8) s'appliquent aux fins de la présente directive.* »

A l'heure actuelle, la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques qui transpose la directive ePrivacy se base en son article 2 lettre (j) sur l'ancienne définition de l'article 2, point c) de la directive 2002/21/CE. Le projet de loi sous avis devrait donc comporter une disposition modificative de la loi modifiée du 30 mai 2005 à ce sujet.

De même, la conformité des autres définitions de l'article 2 de la loi modifiée du 30 mai 2005 à l'article 2 de la directive 2018/1972 devrait être vérifiée et des modifications devraient le cas échéant être apportées.

Par ailleurs, la CNPD constate, à l'instar du Conseil d'Etat, que le point 37 de l'article 2 du

¹⁶⁴ Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »).

projet de loi fait référence à la notion d'« autorités compétentes ». Dans la suite du texte, différents articles du projet de loi évoquent ces « autorités compétentes » sans toutefois apporter des précisions à cet égard.

Or, la Commission nationale est susceptible de faire partie des autorités compétentes, auquel cas certaines dispositions du projet de loi lui seraient applicables, telles que les articles 3, 9 et 13. En vertu du principe de sécurité juridique, elle estime nécessaire que les auteurs du projet de loi clarifient quelles sont les autorités compétentes visées et précisent les compétences et tâches respectives. La CNPD reviendra sur ce point dans ses développements relatifs à l'article 8 du projet de loi.

Ad article 5

L'article 5 paragraphe (2) prévoit que « *les opérateurs et les entreprises offrant des services de communications électroniques mettent d'office et gratuitement à la disposition des autorités compétentes en la matière les données techniques et les équipements permettant à celles-ci l'accomplissement de leurs missions légales de surveillance des communications* ». La CNPD suppose que par « missions légales de surveillance des communications », il faut comprendre les mesures pouvant être ordonnées sur base des articles 67-1 et 88-1 à 88-4 du code de procédure pénale ainsi que de l'article 7, paragraphes (1) et (2) de la loi du 5 juillet 2016 modifiée portant réorganisation du Service de renseignement de l'Etat.

En vertu de la jurisprudence de la Cour européenne des droits de l'homme, toute ingérence dans le droit au respect de la vie privée requiert une loi qui doit être « *accessible aux personnes concernées et prévisible quant à ses répercussions* »¹⁶⁵. 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 »¹⁶⁶. « Le degré de précision requis de la "loi" à cet égard dépendra du sujet en question. »¹⁶⁷.

Pour améliorer le caractère prévisible et précis de la disposition ci-dessus, la CNPD suggère de faire une référence explicite aux textes de loi prévoyant les mesures de surveillance en question.

Il convient en effet d'éviter qu'une disposition légale ne prévoyant pas de manière explicite la surveillance de communications puisse être utilisée à cette fin (par exemple les dispositions du Code de procédure pénale relatives aux perquisitions, diverses dispositions légales accordant des pouvoirs d'investigation à des autorités administratives ou l'article 3 de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État qui définit des missions du Service de renseignement). En effet, les dispositions spécifiques, outre de répondre à l'exigence de prévisibilité de la jurisprudence de la Cour européenne des droits de l'homme, doivent contenir des conditions limitant les mesures de surveillance à un minimum.

¹⁶⁵ 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.

¹⁶⁶ 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.

¹⁶⁷ CouEDH, The Sunday Times c. Royaume-Uni, n° 6538/74, 26 avril 1979, para. 49; voir également 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.

6

ANNEXES

A titre d'exemple, en procédure pénale, un accès judiciaire aux données de connexion (article 67-1 du Code de procédure pénale) ou au contenu de communications électroniques (articles 88-1 et suivants) n'est possible que dans le contexte de faits qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement (article 67-1) respectivement deux ans d'emprisonnement (article 88-2), alors que les dispositions relatives au perquisitions et saisies ne comprennent pas de telles conditions. Par ailleurs, les mesures de surveillance nécessitent l'intervention d'un juge d'instruction, même en cas de crime ou de délit flagrant¹⁶⁸.

Cependant, afin de tenir compte de l'apparition de nouvelles formes de services de communication électronique (offerts par les « over the top players » mentionnés ci-dessus en introduction), couvertes par la définition élargie de l'article 2 paragraphe (4) du projet de loi, la Commission nationale se pose la question de savoir si les dispositions actuelles du Code de procédure pénale (articles 67-1 et 88-1 à 88-4) relatives au contrôle des communications électroniques sont suffisantes ou si, par contre, il faudrait introduire des dispositions spécifiques dans le Code de procédure pénale, voire modifier les dispositions existantes. La CNPD constate par ailleurs que les termes utilisés pour désigner les entreprises devant coopérer avec les autorités ne sont pas uniformisés dans le Code de procédure pénale (« opérateur de télécommunications » et « fournisseur d'un service de télécommunications » à

l'article 67-1¹⁶⁹, « opérateur des postes et télécommunications » à l'article 88-4) et à l'article 5 paragraphe (2) du projet de loi (« opérateurs et les entreprises offrant des services de communications électroniques »).

L'article 5 paragraphe (2) précise par ailleurs qu'« un règlement de l'Institut précise au besoin le format et les modalités de mise à disposition des données techniques et des équipements ».

La CNPD croit comprendre que cette disposition régleme les mesures techniques préalables permettant l'interception des données par les fournisseurs de service ou opérateurs. Par opposition, la transmission des données ainsi obtenues par les fournisseurs de service ou opérateurs aux autorités judiciaires et au Service de renseignement de l'Etat relève de l'article 3 paragraphe (2) du projet de loi n°7424 portant création d'une plateforme commune de transmission électronique sécurisée et modification : 1. du code de procédure pénale, 2. de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat. Cet article prévoit ce qui suit : « *Le format et les modalités d'exécution suivant lesquelles les données collectées au sens des articles 43-1, 67-1 du code de procédure pénale et de l'article 7, paragraphe 2, de la loi du 5 juillet 2016 modifiée portant réorganisation du Service de renseignement de l'Etat sont à transmettre, respectivement aux autorités judiciaires et au Service de renseignement de l'Etat, sont définis par règlement grand-ducal.* ». Ledit projet de loi a fait l'objet de l'avis 40/2019 du 5 juin 2019 de la CNPD¹⁷⁰.

¹⁶⁸ Pour ce qui est de l'article 67-1 du Code de procédure pénale, cf. un arrêt de la Cour d'appel, cinquième chambre, 26 février 2008, arrêt 106/08 V.

¹⁶⁹ L'article 7 paragraphe (2) de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat utilise les mêmes termes.

¹⁷⁰ <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2019/40-plateforme-unique-de-transmission-electronique-securisee.pdf>.

Ad article 8

L'article 8 paragraphe (2) lettre d) prévoit que l'Institut Luxembourgeois de Régulation (ci-après : « l'ILR ») a la charge de « *contribuer à la protection des droits des utilisateurs finaux dans le secteur des communications électroniques en coordination, le cas échéant, avec d'autres autorités compétentes* ».

La CNPD se demande si elle figure parmi les autorités compétentes en question. Elle note aussi que la « coordination » prémentionnée n'est règlementée que par les dispositions sommaires des paragraphes (3) et (4) de l'article 8. Pour des raisons de prévisibilité juridique et afin d'assurer une coordination efficace entre autorités compétentes, la Commission nationale estime nécessaire, d'une part, de nommer dans le projet de loi les autorités compétentes en la matière ainsi que de clarifier leurs compétences et tâches respectives, et d'autre part, de préciser les modalités d'une telle coordination.

Ad article 19

L'article 19 énumère les obligations dont est assortie l'autorisation générale, obligations à charge des entreprises qui fournissent un réseau ou un service de communications électroniques à l'exception des services de communications interpersonnelles non fondés sur la numérotation.

L'article 19 paragraphe (1) 4° prévoit « *la facilitation de l'interception légale par les autorités nationales compétentes, conformément au*

règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et à la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ».

Comme elle l'a mentionné précédemment à propos de l'article 5, la CNPD estime qu'il serait préférable que l'article 19 paragraphe (1) 4° se réfère à des dispositions précises du Code de procédure pénale et de la loi du 5 juillet 2016 modifiée portant réorganisation du Service de renseignement de l'Etat, afin d'améliorer le caractère prévisible de la loi au sens de la jurisprudence de la Cour européenne des droits de l'homme.

La CNPD note également que l'article 19 paragraphe (1) 4° ne s'applique pas aux services de communications interpersonnelles non fondés sur la numérotation alors que l'article 5 paragraphe (2) traitant également la coopération des entreprises aux mesures de surveillance ordonnées par les autorités est d'application générale. Elle se demande si cette différence de traitement est voulue.

Ad article 33

L'article 33 prévoit les sanctions que l'ILR peut infliger à des entreprises ne respectant pas certaines dispositions du projet de loi.

6

ANNEXES

La CNPD se demande si cet article 33 ne pourrait pas engendrer en pratique un risque de procédures administratives parallèles pouvant aboutir à des sanctions devant l'ILR et la CNPD pour les mêmes faits.

On peut songer à des faits constituant à la fois une violation de l'article 42 du projet de loi et de l'article 32 du RGPD, articles mettant des obligations de sécurité à charge des entreprises. De même, un fait constituant une violation du secret des correspondances viole aussi bien l'article 19 paragraphe (1) point 2 du projet de loi que l'article 4 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques. En effet, en vertu de l'article 12 de la loi modifiée du 30 mai 2005, la Commission nationale pour la protection des données est chargée d'assurer l'application des dispositions de ladite loi du 30 mai 2005 et de ses règlements d'exécution. On peut également penser à certaines violations de l'article 10 bis de la loi modifiée du 30 mai 2005. En effet, l'article 33 paragraphe (4) du projet sous avis mentionne expressément ledit article 10 bis parmi les dispositions légales dont la violation peut donner lieu à une amende d'ordre par l'ILR. Or, en vertu de l'article 12 précité de la loi modifiée du 30 mai 2005, la CNPD est chargée d'assurer l'application dudit article 10 bis.

Plusieurs questions se posent à ce sujet.

Serait-il indiqué qu'une autorité suspende une procédure pouvant aboutir à une sanction quand elle a connaissance de la procédure parallèle devant l'autre autorité ?

En l'absence de procédure d'échange d'information réglementée de manière précise, il se pose aussi la question de savoir comment une des deux autorités aura connaissance qu'une procédure est en cours devant l'autre autorité.

Est-ce que l'autorité qui est ou s'est saisie la première devrait en informer l'autre autorité ?

Si on admet qu'un même fait peut donner lieu à ces procédures devant les deux autorités, est-ce qu'un même fait peut alors également donner lieu à des sanctions administratives à la fois par l'ILR ou la CNPD, ou par contre, une telle double sanction administrative devrait-elle être exclue d'office à l'image du principe non bis in idem existant en droit pénal ? La CNPD estime dès lors nécessaire de clarifier cette problématique dans le projet de loi.

Ad article 43

L'article 43 paragraphe (5) prévoit une coopération entre l'ILR et de la CNPD dans le domaine de la sécurité des réseaux et services dans les termes suivants :

« En fonction des besoins et conformément au droit national, l'Institut consulte les autorités judiciaires compétentes, la Commission de surveillance du secteur financier, et la Commission nationale pour la protection des données et coopère avec elles. »

La CNPD se demande quelles formes pourra prendre la coopération prévue par cet article.

S'agit-il seulement de coordonner les positions des deux autorités sur des questions de principe touchant à la sécurité des communications et des traitements? Ou peut-il y avoir une coopération sur des affaires dont une des autorités est saisie, par exemple dans le cadre de procédures de sanction de l'article 33 mentionnées ci-dessus. Une telle coopération impliquerait un échange d'informations sur des dossiers entre l'ILR et la CNPD, informations qui sont protégées par le secret professionnel.

Ad Article 112

L'article 112 reprend l'article 100 de la directive (UE) 2018/1972 qui impose le respect des droits fondamentaux dans le secteur des communications électroniques.

La CNPD tient à rendre attentif au fait que cette disposition de la directive doit non seulement être inscrite dans un article de la loi de transposition, mais que, par ailleurs, les dispositions légales nationales applicables et la pratique doivent respecter les principes établis dans la directive et ne pas entrer en contradiction avec ladite loi.

Ceci vaut en particulier pour le secret des communications protégé notamment par l'article 7 de la Charte des droits fondamentaux de l'Union européenne.

A l'heure actuelle, le secret des communications en matière de communications électroniques est notamment protégé au niveau national par la loi modifiée du 30 mai 2005 concernant la

protection de la vie privée dans le secteur des communications électroniques et en particulier par l'article 4 de cette loi.

Cependant, à l'heure actuelle, la définition du « *service de communications électroniques* » de l'article 2 lettre (j) de la loi modifiée du 30 mai 2005 précitée est plus étroite que celle de l'article 2 paragraphe (4) du projet de loi qui englobe aussi les « *over the top players* ». Comme il a été expliqué ci-dessus dans le commentaire relatif à l'article 2 projet de loi, et conformément à l'article 125 troisième alinéa de la directive (UE) 2018/1972, les définitions de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques devraient être adaptées pour être conformes à l'article 2 de la directive (UE) 2018/1972.

A défaut, il y aurait un risque que certaines nouvelles formes de communications électroniques ne soient pas couvertes par les dispositions relatives au secret des correspondances de la loi modifiée du 30 mai 2005, du moins aussi longtemps que le futur Règlement « ePrivacy » n'est pas adopté et en vigueur.

Ad article 124

L'article 124 paragraphe (5) tend à garantir une localisation rapide de l'auteur d'un appel d'urgence.

La CNPD note qu'à l'heure actuelle, la question de la localisation des appels d'urgence est

6

ANNEXES

traitée par l'article 7 paragraphe (5) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

D'ailleurs, une modification dudit article 7 est en cours d'être effectuée par 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. Ledit projet de loi a fait l'objet de l'avis 11/2020 du 24 avril 2020 de la CNPD⁷¹. Cette modification tend à permettre la localisation des appels via des informations obtenues à partir de l'appareil mobile de l'appelant (c'est-à-dire en particulier via des informations de localisation par le système mondial de navigation par satellite (GNSS) ou via un réseau Wifi).

La CNPD comprend que l'article 124 paragraphe (5) projeté complète l'article 7 précité de la loi modifiée du 30 mai 2005 qui reste en vigueur après l'entrée en vigueur de la loi projetée sous avis. Elle estime nécessaire de préciser dans le projet de loi comment cette disposition s'articule avec la modification apportée par le projet de loi n°7526.

Ad article 131

L'article 131 du projet de loi régit les factures détaillées.

Pour ce qui est des appels gratuits, le paragraphe (2) alinéa 4 dispose ce qui suit: « *Les appels qui sont gratuits pour l'utilisateur final appelant, y compris les appels aux lignes d'assistance, ne doivent pas nécessairement être indiqués sur la facture détaillée de l'utilisateur final appelant* ». Cet alinéa laisse un choix – apparemment au bénéfice du fournisseur de service et non au client – d'inclure ou de ne pas inclure ces appels dans les factures détaillées.

Ceci contredit l'actuel article 6 paragraphe (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, paragraphe qui reste en vigueur et qui dispose ce qui suit: « *Les appels gratuits y compris ceux aux lignes d'assistance ne sont pas indiqués sur la facture détaillée indépendamment de son degré de détail.* » Une clarification s'impose dès lors dans le projet de loi.

Ad article 132

L'article 132 paragraphes (1) et (2) régit l'identification de la ligne d'appel.

La CNPD comprend que l'article 132 paragraphes (1) et (2) projeté complète les paragraphes (1) à (4) de l'article 7 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, paragraphes qui resteront en vigueur après l'entrée en vigueur de la loi projetée sous avis. Les auteurs du projet de loi devraient donc clarifier

⁷¹ <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2020/11-communication-electroniques-PL7526.pdf>

l'articulation du projet de loi sous avis avec les dispositions de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Ainsi décidé à Belvaux en date du 3 mars 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

**Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n° 7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.
(Délibération n°8/AV7/2021 du 3/03/2021)**

Conformément à l'article 46, paragraphe 1^{er}, 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 1^{er} 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 1^{er} 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 ».

Le 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 »)¹⁷².

En date du 17 avril 2020, la Commission nationale a rendu son avis complémentaire sur l'amendement gouvernemental au projet de loi, approuvé par le Conseil de gouvernement dans sa séance du 20 mars 2020¹⁷³.

Le 19 novembre 2020, la Commission de la Sécurité intérieure et de la Défense a adopté une série d'amendements relative au projet de loi (ci-après les « amendements »).

Dans la mesure où les amendements concernent des dispositions qui ont été commentées par la CNPD dans ses avis précités des 28 février et 17 avril 2020, celle-ci s'autosaisit pour les aviser.

1. Sur les amendements adoptés par la Commission de la Sécurité intérieure et de la Défense

- Ad Amendement 1

L'Amendement 1 a pour objet de modifier le paragraphe (1) de l'article 43bis nouveau de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale. Cette modification consiste en l'ajout des finalités « *telles qu'elles figuraient à l'article 17, paragraphe 1^{er}, lettre (a) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* »¹⁷⁴.

La Commission nationale accueille favorablement cet ajout alors qu'elle l'avait suggéré dans

¹⁷² Avis de la Commission nationale pour la protection des données 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.

¹⁷³ Avis complémentaire de la Commission nationale pour la protection des données 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.

¹⁷⁴ Commentaire des auteurs du projet de loi sous « Amendement 1 », document parlementaire n°7498/06, page 1.

son avis du 28 février 2020 relatif au projet de loi¹⁷⁵, à l'instar du Conseil d'Etat dans son avis du 10 mars 2020¹⁷⁶.

En ce qui concerne le remplacement des termes « *risque particulier de commission de crimes ou délits ou d'atteintes à la sécurité des personnes ou des biens* » par la notion de « *risque particulier de commission d'infractions pénales* », il y a lieu de relever que cette modification reprend sensiblement les termes de l'article 17, paragraphe (1) lettre d) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel¹⁷⁷.

Cette modification est guidée par l'intention des auteurs du projet de loi de ne pas « *limiter la vidéosurveillance à des catégories particulières d'infractions* ». Cependant, ces derniers semblent vouloir exclure les contraventions du champ d'application du projet de loi sous avis.

En effet, les auteurs du projet de loi précisent que « *[l]'utilisation des termes « infractions pénales », qui englobent celles qualifiées de contraventions, ne signifie en aucun cas que l'intention est d'étendre la vidéosurveillance à des lieux où des contraventions sont commises* »¹⁷⁸.

Si la volonté des auteurs du projet de loi n'est pas d'étendre la vidéosurveillance à des lieux où des contraventions seraient commises, il y a lieu de s'interroger sur la pertinence de la terminologie employée. Dès lors, ne faudrait-il pas reprendre la proposition du Conseil d'état dans son avis du 10 mars 2020 en ce qu'il propose de se référer aux termes « crimes ou délits »¹⁸⁰ ?

Enfin, dans la mesure où le changement de terminologie entraîne un élargissement du champ d'application de la vidéosurveillance, la CNPD se permet d'insister sur l'importance que revêt l'analyse d'impact qui devrait être effectuée notamment en ce qui concerne la justification de la nécessité de la vidéosurveillance au regard des critères définis au paragraphe (2) de l'article 43bis nouveau et des finalités poursuivies.

- **Ad Amendement 2**

En ce qui concerne le remplacement des termes « *de crimes ou délits ou d'atteintes à la sécurité des personnes ou des biens* » par les mots « infractions pénales », la CNPD renvoie à ses commentaires ci-avant.

La Commission nationale accueille favorablement les autres modifications mais tient néanmoins à réitérer ses commentaires

¹⁷⁵ Avis de la Commission nationale pour la protection des données 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, page 5.

¹⁷⁶ Avis du Conseil d'Etat du 10 mars 2020 relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, document parlementaire n°7498/01, page 2.

¹⁷⁷ Article 17 paragraphe (1) lettre d) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel dispose que « [l]'ont l'objet d'un règlement grand-ducal : la création et l'exploitation, aux fins et conditions visées sous (a), d'un système de vidéosurveillance des zones de sécurité. Est à considérer comme telle tout lieu accessible au public qui par sa nature, sa situation, sa configuration ou sa fréquentation présente un risque accru d'accomplissement d'infractions pénales. Les zones de sécurité sont fixées dans les conditions prévues par règlement grand-ducal ».

¹⁷⁸ Commentaire des auteurs du projet de loi sous « Amendement 1 », document parlementaire n°7498/06, page 2.

¹⁷⁹ Commentaire des auteurs du projet de loi sous « Amendement 1 », document parlementaire n°7498/06, page 2.

¹⁸⁰ Avis du Conseil d'Etat du 10 mars 2020 relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, document parlementaire n°7498/01, page 3.

6

ANNEXES

formulés dans son avis complémentaire du 17 avril 2020 relatif au projet de loi¹⁸¹ en ce qu'elle suggère, à l'instar du Conseil d'Etat¹⁸², la suppression du point 4° du paragraphe (2) de l'article 43bis nouveau de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

- Ad Amendement 3

La Commission nationale se félicite que les auteurs du projet de loi aient remplacé le terme « zone de sécurité » par « lieu », tel qu'elle l'avait suggéré dans son avis complémentaire du 17 avril 2020 relatif au projet de loi¹⁸³, à l'instar du Conseil d'Etat¹⁸⁴.

- Ad Amendement 4

Il y a lieu de féliciter les auteurs du projet de loi quant aux modifications apportées à l'article 43bis nouveau, paragraphe (5), alinéa 2, en ce que ces dispositions prévoient que « *[l]e recours à des techniques de reconnaissance faciale est exclu* ».

Les auteurs du projet de loi ont notamment suivi la suggestion faite par la CNPD dans son avis du 28 février 2020 relatif au projet de loi. La Commission nationale regrette toutefois que le texte sous avis ne reprenne pas sa suggestion concernant l'exclusion du captage des sons¹⁸⁵.

Par ailleurs, les auteurs du projet de loi précisent encore dans leur commentaire de l'amendement sous avis que « *[l]interdiction du recours à des techniques de reconnaissance faciale n'est donc pas à comprendre comme une interdiction générale et n'implique notamment pas que ces techniques ne puissent pas être utilisées dans le contexte de la poursuite pénale pour élucider des infractions pénales d'après les règles de la procédure pénale* ».

A ce sujet, il convient d'attirer l'attention des auteurs du projet de loi sur le fait que 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.

- Ad Amendement 5

La CNPD salue le fait que les auteurs du projet de loi aient intégré les propositions faites dans son avis du 28 février 2020 relatif au projet de loi en ce qui concerne le paragraphe (6) de l'article 43bis nouveau de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

- Ad Amendement 6

Cet amendement a notamment pour objet de supprimer la référence faite à « *[l]a Police*

¹⁸¹ Avis complémentaire de la Commission nationale pour la protection des données 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, pages 1 et 2.

¹⁸² V. avis complémentaire du Conseil d'Etat du 12 mai 2020 relatif au projet de loi n° 7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, document parlementaire n°7498/04, page 2 et deuxième avis complémentaire du Conseil d'Etat du 23 février 2021 relatif au projet de loi n° 7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, page 3.

¹⁸³ Avis complémentaire de la Commission nationale pour la protection des données 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, pages 2 et 3.

¹⁸⁴ Avis complémentaire du Conseil d'Etat du 12 mai 2020 relatif au projet de loi n° 7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, document parlementaire n°7498/04, page 2.

¹⁸⁵ Avis de la Commission nationale pour la protection des données 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, page 7.

grand-ducale, représentée par son directeur général » en sa qualité de responsable du traitement.

Cette suppression intervient « [à] la lumière des travaux d'élaboration d'une base légale spécifique relative aux traitements de données à caractère personnel effectués par la Police grand-ducale »¹⁸⁶.

En effet, il y a lieu de relever que l'article 4 du projet de loi n°7741 insère un nouvel article 43-3 dans la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, qui désigne la Police grand-ducale comme responsable du traitement pour les traitements de données à caractère personnel qu'elle effectue.

- Ad Amendement 7

Cet amendement complète le paragraphe (9) de l'article 43bis nouveau en ce qu'il prévoit que les données ne seraient pas effacées après un délai de deux mois pour les cas visés au nouveau paragraphe (11), introduit par ledit amendement.

Ce nouveau paragraphe (11) de l'article 43bis nouveau dispose que « [l]e traitement de données à caractère personnel aux fins de la prévention, de la recherche et de la constatation d'infractions pénales peut être utilisé par la Police à des fins d'analyses de déroulement des opérations, y compris l'examen d'incidents ayant comme objectif l'amélioration des plans et procédures d'intervention, ainsi qu'à des fins de formation interne ».

La Commission nationale note l'introduction d'une telle finalité dans une base légale ce qui est en effet nécessaire conformément à l'article 8, paragraphe (1) de la loi du 1^{er} 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.

A la lecture du commentaire de l'amendement sous avis, la Commission nationale comprend que les « *images enregistrées* » seraient utilisées par la Police grand-ducale pour « *effectuer l'analyse du déroulement de l'intervention, ainsi que pour des fins de formation interne, dans le but d'améliorer les plans et procédures des interventions futures du même type* ».

Cependant, comme relevé par le Conseil d'Etat dans son deuxième avis complémentaire du 23 février 2021 « *l'emploi des termes « [l]e traitement de données à caractère personnel aux fins de la prévention, de la recherche et de la constatation d'infractions pénales* » prête à croire que l'ensemble des données utilisées par la Police grand-ducale aux fins de la prévention, de la recherche et de la constatation d'infractions pénales pourraient être utilisées aux autres finalités y énoncées. Une telle disposition, outre le fait qu'elle ne concorde pas avec l'intention des auteurs telle qu'explicitée au commentaire de l'amendement, dépasserait l'objet de la loi en projet »¹⁸⁷.

La CNPD se rallie encore aux interrogations soulevées par le Conseil d'Etat en ce qu'il se

¹⁸⁶ Commentaire des auteurs du projet de loi sous « Amendement 6 », document parlementaire n°7498/06, page 5.

¹⁸⁷ Deuxième avis complémentaire du Conseil d'Etat du 23 février 2021 relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, document parlementaire n°7498/08, page 5.

6

ANNEXES

« demande s'il est nécessaire de recourir à l'ensemble des données recueillies à travers la vidéosurveillance ou s'il ne suffirait pas de viser les seules données relatives à des interventions policières d'envergure et présentant un intérêt dans le cadre de l'analyse du déroulement de l'intervention et de la formation interne »¹⁸⁸.

Par ailleurs, en l'absence de précisions quant aux mesures techniques qui seraient prises (par exemple technique de masquage ou de floutage des visages des personnes concernées) afin d'utiliser les images issues de la vidéosurveillance « à des fins d'analyses de déroulement des opérations, y compris l'examen d'incidents ayant comme objectif l'amélioration des plans et procédures d'intervention, ainsi qu'à des fins de formation interne », la Commission nationale n'est pas en mesure d'apprécier si le principe de minimisation des données est respecté en l'espèce.

Les auteurs du projet de loi devraient, dès lors, préciser quelles seraient les données qui seraient consultées pour les finalités prévues au paragraphe (11) de l'article 43bis nouveau ainsi que les moyens techniques qui seraient pris afin de réutiliser les images issues de la vidéosurveillance pour de telles finalités.

A titre de comparaison, il est intéressant de noter qu'en Belgique, l'article 25/7 paragraphe (2) de la loi modifiée sur la fonction de police du 5 août 1992 dispose qu'« [a]près anonymisation, les données à caractère personnel et informations visées au

paragraphe 1^{er} peuvent être utilisées à des fins didactiques et pédagogiques dans le cadre de la formation des membres des services de police ».

Il convient de noter que l'anonymisation des données à caractère personnel a comme conséquence qu'une fois anonymisées, les données ne sont plus soumises au RGPD et leur diffusion ou leur réutilisation n'a pas d'impact sur la vie privée des personnes concernées.

Si l'intention des auteurs du projet de loi n'est pas de prévoir que les données soient anonymisées, la Commission nationale regrette que la durée de conservation des images pour les finalités indiquées au paragraphe (11) de l'article 43bis nouveau n'ait pas été précisée.

Il y a lieu de rappeler que 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. Au-delà, les données doivent être supprimées ou anonymisées.

Or, en l'absence de telles précisions dans le projet de loi sous avis, la Commission nationale n'est pas en mesure d'apprécier si ce principe est respecté.

Dès lors, la CNPD estime que la durée de conservation devrait être définie dans le projet de loi ou que celui-ci devrait *a minima* préciser les critères qui seraient pris en compte afin de déterminer quelle est la durée de conservation

¹⁸⁸ Deuxième avis complémentaire du Conseil d'Etat du 23 février 2021 relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, document parlementaire n°7498/08, page 5.

proportionnée pour les données issues de la vidéosurveillance et traitées pour les finalités énoncées au paragraphe (1) de l'article 43bis nouveau.

2. Sur l'avis du Syndicat des villes et communes luxembourgeoises¹⁸⁹

Il est renvoyé aux développements de la CNPD dans son avis du 28 février 2020 et ses avis du 15 mars 2019 relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique (délibération n° 36/2019) et du 10 mai 2019 relatif au recours de la vidéosurveillance par les communes (délibération n°39/2019) sur la nécessité de l'introduction d'un cadre légal permettant à une commune qui souhaite installer, en tant que responsable du traitement, un dispositif de vidéosurveillance dans les espaces publics à des fins de sécurité publique, incluant de façon générale la sécurité des personnes et des biens.

La Commission nationale renvoie encore à ses avis du 28 février 2020 et des 15 mars et 10 mai 2019 précités en ce qui concerne les interactions entre la police et les bourgmestres alors que ni la loi communale du 13 décembre 1988 ni la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ne précisent les compétences des bourgmestres en matière de police administrative.

Enfin, il y a lieu de relever que le projet de loi sous examen prévoit actuellement que seul 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. Dans l'hypothèse où ledit système serait étendu à d'autres territoires communaux, ne faudrait-il pas prévoir un système qui ne reposerait pas que sur la seule initiative du directeur général de la Police grand-ducale ?

La CNPD se demande si l'initiative de placer sous surveillance un lieu ou espace public ne pourrait pas être prise également à l'initiative du bourgmestre territorialement compétent, tel que suggéré par le Syndicat des villes et communes luxembourgeoises dans son avis du 25 janvier 2021 relatif au projet de loi¹⁹⁰. Néanmoins, la Commission nationale émet des réserves quant à la proposition de reformulation de l'article 43bis nouveau, paragraphe (1), faite par le SYVICOL dans son avis précité alors que ni la loi communale précitée, ni la loi sur la Police grand-ducale précitée ne précisent les compétences des bourgmestres en matière de police administrative.

La CNPD souligne encore une fois que VISUPOL est un système de vidéosurveillance opéré par la Police grand-ducale en tant que responsable du traitement, qui n'aura pas, a priori, vocation à être étendu à d'autres territoires communaux que celui de la Ville de Luxembourg et que la problématique de la licéité de la surveillance par caméras vidéo d'espaces ou de lieux publics effectuée à l'initiative des Communes n'est pas résolue

¹⁸⁹ Avis du Syndicat des villes et communes luxembourgeoises du 25 janvier 2021, relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, document parlementaire n°7498/07.

¹⁹⁰ Avis du Syndicat des villes et communes luxembourgeoises du 25 janvier 2021, relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, document parlementaire n°7498/07, page 2.

6

ANNEXES

par le projet de loi sous examen. Dès lors, la Commission nationale ne peut que réitérer ses observations formulées dans ses avis du 15 mars 2019 relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique (délibération n° 36/2019) et du 10 mai 2019 relatif au recours de la vidéosurveillance par les communes (délibération n°39/2019).

Ainsi décidé à Belvaux en date du 3 mars 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 janvier 2021, Monsieur le Ministre de la Sécurité sociale a saisi la Commission nationale d'une demande d'avis sur le projet de loi n°7751 modifiant 1° le Code de la sécurité sociale ; 2° le Code du travail ; 3° la loi modifiée du 15 décembre 1993 déterminant le cadre du personnel des administrations, des services et des juridictions de la sécurité sociale; et 4° la loi modifiée du 28 juillet 2000 ayant pour objet la coordination des régimes légaux de pension (ci-après : « projet de loi n°7751 »).

D'après l'exposé des motifs, le projet de loi n°7751 a pour objet d'apporter des corrections au Code de la sécurité sociale pour différentes raisons, dont notamment la mise à jour des

**Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7751 modifiant 1° le Code de la sécurité sociale ; 2° le Code du travail ; 3° la loi modifiée du 15 décembre 1993 déterminant le cadre du personnel des administrations, des services et des juridictions de la sécurité sociale; et 4° la loi modifiée du 28 juillet 2000 ayant pour objet la coordination des régimes légaux de pension.
(Délibération n°8/AV8/2021 du 03/03/2021)**

renvois à d'autres lois, le redressement d'erreurs matérielles ou des adaptations nécessaires suite à l'entrée en vigueur d'autres lois ayant un impact sur la législation de sécurité sociale, telle que la loi du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière. Par ailleurs, les auteurs du projet de loi précisent que « *conformément au souhait de la Commission nationale pour la protection des données, les dispositions concernant la durée de conservation des données traitées dans le dossier de soins partagé, qui figurent actuellement dans un règlement grand-ducal, sont intégrées dans la loi à l'article 60quater du Code de la sécurité sociale.* »

La Commission nationale entend ainsi limiter ses observations aux dispositions du projet de loi n°7751 ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel, et plus particulièrement son article 1^{er} point 19 qui vise précisément à modifier l'article 60quater précité du Code de la sécurité sociale.

Ad article 1^{er} point 19 du projet de loi n°7751

Actuellement, la durée de conservation des données versées dans le dossier de soins

6

ANNEXES

partagé est prévue par l'article 10 paragraphe (5) du règlement grand-ducal du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé.

L'article 1^{er} point 19 du projet de loi n°7751 sous avis « *a pour objet d'inscrire le principe de la durée de conservation des données traitées avec les dérogations garantissant une flexibilité, tel que retenu au moment de l'élaboration du règlement grand-ducal, dans l'article 60quater du Code de la sécurité sociale.* »¹⁹¹

Déjà dans son avis du 5 avril 2018 relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé, la CNPD avait considéré qu'au vu 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 européenne¹⁹², les dispositions concernant la durée de conservation des données au DSP devraient être prévues dans la loi au sens stricte du terme et plus précisément par l'article 60quater du Code de la sécurité sociale, et non pas dans un acte réglementaire.

De manière générale, la CNPD ne peut donc que soutenir la modification susmentionnée visant à insérer un paragraphe (6) à l'article 60quater du Code de la sécurité sociale sur la durée de conservation des données versées

dans le dossier de soins partagé. Néanmoins, elle constate que les deux derniers alinéas de l'article 10 paragraphe (5) du règlement grand-ducal du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé n'ont pas été repris par les auteurs du projet de loi n°7751. Ainsi, la CNPD leur recommande de compléter le nouveau paragraphe (6) de l'article 60quater du Code de la sécurité sociale par les deux alinéas suivants :

« L'accord du titulaire est daté et consigné dans son espace d'expression personnelle dans l'application dossier de soins partagé.

Par dérogation à l'alinéa 1^{er}, les informations relatives à l'expression personnelle du titulaire du dossier de soins partagé sont conservées jusqu'à ce que ce dernier les modifie ou les supprime. »

Finalement, dans son avis précité du 5 avril 2018, la CNPD avait estimé que sur base des principes susmentionnés, les dispositions réglementant les droits des titulaires mineurs non émancipés et titulaires majeurs protégés par la loi devraient aussi être prévues dans la loi au sens stricte du terme et plus précisément par l'article 60quater du Code de la sécurité sociale, et non pas dans un acte réglementaire.

Dans son avis complémentaire du 18 octobre 2019 relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé,¹⁹³ la Commission nationale avait constaté que les

¹⁹¹ Voir commentaire de l'article 1er point 19 du projet de loi n°7751.

¹⁹² Pour plus de détails, la CNPD renvoie à sa délibération n° 242/2018 du 5 avril 2018.

¹⁹³ Délibération n° 51/2019 18 octobre 2019.

auteurs dudit projet avaient tout simplement supprimé l'ancien article 7 du projet de règlement grand-ducal concernant les titulaires mineurs non émancipés et titulaires majeurs protégés par la loi pour les raisons suivantes : « *Les avis du Conseil d'Etat et de la Commission nationale pour la protection des données établissent que l'article 7, du moins en partie, déroge aux règles relatives aux mineurs et aux majeurs protégés par la loi telles que prévues au Code civil.*

Ainsi dans un souci du respect de la hiérarchie des normes, l'article 7 est supprimé, les dispositions qui introduisent des droits spécifiques pour certains mineurs devant être reprises dans les lois particulières régissant leurs droits. »

Or, sauf erreur de sa part, la CNPD constate qu'aucun projet de loi n'ait été déposé à la Chambre des Députés, en vue d'adopter les

mesures législatives nécessaires pour prendre en compte lesdites considérations sur les droits des titulaires mineurs non émancipés et titulaires majeurs protégés par la loi. Elle se demande dès lors pourquoi les auteurs du projet de loi n°7751 n'ont pas profité du projet de loi sous examen pour introduire les mesures législatives en question.

Ainsi décidé à Belvaux en date du 3 mars 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

**Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7784 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19.
(Délibération n°10/AV9/2021 du 8/03/2021)**

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 5 mars 2021, Madame la Ministre de la Santé a saisi la Commission nationale d'une demande d'avis sur le projet de loi n°7784 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 (ci-après le « projet de loi n°7784 »).

Il ressort de l'exposé des motifs que le présent projet de loi vise à maintenir les restrictions actuellement en place jusqu'au 2 avril 2021 inclus, tout en créant « *une base légale pour l'application des mesures temporaires pouvant être prises dans le cadre de la lutte contre la pandémie Covid 19 au niveau de l'enseignement national et en ce qui concerne les mesures de réorganisation et de suspension ayant un impact sur les structures d'accueil pour enfants.* »

La CNPD constate en effet que l'article 3 du projet de loi n°7784 prévoit d'insérer un nouvel article 4^{ter} dans la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 listant dans son paragraphe 1^{er} toute une série de mesures temporaires qui peuvent être prises dans le cadre de la lutte contre la pandémie Covid-19, en présence d'une recrudescence locale ou nationale des infections comportant des risques sanitaires pour la population locale ou globale avec des chaînes d'infections importantes dans les structures visées au paragraphe 2 dudit article 4^{ter}. Une de ces mesures¹⁹⁴ constitue le passage à un enseignement à distance pour une partie ou pour l'ensemble des établissements scolaires publics et privés tels que définis aux points 1 et 2 du paragraphe 2 du nouvel article 4^{ter} de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19.

De manière générale, la CNPD félicite les auteurs du projet de loi n°7784 sous examen d'avoir créé une base légale permettant, sous certaines conditions, le passage à un

¹⁹⁴ Comme prévu par le point 2° du paragraphe 1^{er} du nouvel article 4^{ter} de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19.

enseignement à distance pour une partie ou pour l'ensemble des établissements scolaires publics et privés. Elle regrette pourtant que le projet de règlement grand-ducal prévu au nouvel article 4^{ter} paragraphe (3) de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19, qui devrait déterminer les « *mesures temporaires prises en application des conditions prévues au paragraphe 1^{er} du présent article, la durée de leur application, ainsi que les structures et les activités visées par l'application desdites mesures* », ne soit pas joint au présent projet de loi de sorte que la CNPD n'est pas en mesure d'en apprécier l'impact sur d'éventuelles dispositions en matière de protection des données.

Elle s'interroge par ailleurs qui décidera concrètement de la mise en place de ces mesures. Est-ce que ce sera le Ministre de la Santé ou, le cas échéant, le Ministre de l'Education nationale, de l'Enfance et de la Jeunesse ?

Finalement, la CNPD regrette que les auteurs du projet de loi n°7784 n'ont pas pris en compte les commentaires formulés dans son avis du 16 février 2021 relatif au projet de loi n°7768 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19.¹⁹⁵

Ainsi décidé à Belvaux en date du 8 mars 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

¹⁹⁵ Délibération n°5/AV4/2021 du 16 février 2021 : <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2021/Avis-05-AV4-2021-du-16-fevrier-2021-PL7768-modifiant-la-loi-Covid.pdf>

6

ANNEXES

**Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7741 portant modification 1° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ; 2° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 3° du Code pénal.
(Délibération n°10/AV10/2021 du 16/03/2021)**

Introduction

1. Conformément à l'article 8 de loi du 1^{er} 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 1^{er} août 2018 portant organisation de la CNPD* »), transposant l'article 46, paragraphe 1^{er}, lettre (e) 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* »), dans le cadre de la loi du 1^{er} 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 (ci-après la « *la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale* », la Commission nationale pour la protection des données (ci-après désignée
2. Par courrier en date du 18 décembre 2020, Monsieur le Ministre de la Sécurité intérieure a invité la Commission nationale à aviser le projet de loi n° 7741 portant modification 1° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ; 2° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; et 3° du Code pénal. En date du 30 décembre 2020, le projet de loi a été déposé à la Chambre des Députés.
3. En 2019, la CNPD a été sollicitée par Monsieur le Ministre de la Sécurité intérieure pour rendre un avis au sujet du fichier central de la Police grand-ducale au regard de la législation en matière de protection des données¹⁹⁶.
4. Selon l'exposé des motifs, le projet de loi « a pour objet d'encadrer les traitements des données à caractère personnel effectués dans les fichiers de la Police grand-ducale, et plus précisément dans le fichier central. Il vise à adresser les critiques en matière de protection des données qui ont été soulevées par rapport aux fichiers de la Police, et plus particulièrement par rapport au fichier central en été 2019 ».

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* ».

¹⁹⁶ Avis de la Commission nationale pour la protection des données relatif au fichier central de la Police grand-ducale au regard de la législation sur la protection des données, Délibération n° 45/2019 du 13 septembre 2019.

1. L'accès à des fichiers d'autres administrations

5. La CNPD note avec intérêt que le projet de loi comporte une mise à jour de la disposition existante concernant l'accès à des traitements de données à caractère personnel mis en œuvre par d'autres administrations étatiques.
6. L'article 1^{er} du projet de loi propose de remplacer l'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale par l'article 43 nouveau reprenant une grande partie de la disposition existante, tout en la mettant à jour sur certains points. L'article 43 nouveau règle l'accès direct, par un système informatique, par des membres de la Police grand-ducale à un certain nombre de bases de données étatiques. Comparé à l'article 43 en vigueur, les auteurs du projet de loi proposent d'étendre l'accès direct aux traitements de données suivants :
 - le registre foncier ;
 - le registre des bénéficiaires effectifs ;
 - le registre public des bâtiments de plaisance battant pavillon luxembourgeois ;
 - le système électronique central de recherche de données concernant des comptes de paiement et des comptes bancaires identifiés par un numéro IBAN et des coffres-forts tenus par des établissements de crédit au Luxembourg ; et
 - le registre des fiducies et des trusts.
7. La CNPD soulève que l'exposé des motifs et le commentaire des articles restent muets

sur la nécessité et la proportionnalité de « l'accès direct, par un système informatique », à ces traitements de données. La CNPD note également que, en termes de protection des données, il y a une différence notable entre un « accès direct, par un système informatique » et la notion de « recevoir sans délai », via un accès différé. Les deux transmissions de données d'un responsable de traitement à un autre peut se faire par voie d'un système informatique. Ce système peut fonctionner par un accès direct, sans intervention du responsable du traitement, ou « sur demande », avec l'intervention du responsable du traitement de données auquel le système informatique permet d'accéder. Or, lors de la mise en place d'un accès direct, le responsable de traitement gérant le registre en question n'intervient *a priori* plus sur les accès effectués par la Police grand-ducale et, par conséquent, il perd en quelque sorte la « maîtrise » sur les données pour lesquelles il est responsable. En particulier pour les traitements nouvellement intégrés dans la liste pour lesquelles la législation correspondante ne prévoit pas explicitement un tel accès, l'absence de justification dans l'exposé des motifs ou dans le commentaire des articles rend impossible d'apprécier si cet accès est nécessaire et proportionnel et si cet accès doit être « direct, par un système informatique ». La Commission nationale ne peut donc pas évaluer si ces accès sont nécessaires dans une société démocratique, sous réserve du principe de proportionnalité et de nécessité.

6

ANNEXES

8. La CNPD regrette que le projet de règlement grand-ducal visé à l'article 43, paragraphe 5, tel que prévu par l'article 1^{er} du projet de loi n'a pas été communiqué en même temps que le projet de loi alors que cet acte réglementaire est déjà prévu, dans des termes identiques, dans l'article 43, alinéa 3, existant. À cet égard, la CNPD rappelle que, dans son avis relatif au projet de loi n° 7045 portant réforme de la Police grand-ducale¹⁹⁷ ayant abouti à ladite loi modifiée du 18 juillet 2018, elle avait déjà estimé qu'il « *aurait été judicieux de joindre en même temps un projet de règlement grand-ducal* » et qu'en l'absence d'un tel texte, la CNPD « *n'est pas en mesure d'apprécier la nécessité et la proportionnalité des données accédées* ».
9. Les bases de données visées à l'article 43 sont créées et maintenues par d'autres administrations en application de législations et de réglementations spécifiques. Ces dispositions législatives et réglementaires continuent d'encadrer les traitements de données à caractère personnel et peuvent prévoir des conditions spécifiques concernant l'accès par les membres de la Police grand-ducale.
10. Ainsi, il semble évident que la présente disposition n'altère en rien les dispositions existantes régissant ces traitements de données, mais confère le droit aux personnes autorisées à y accéder dans la limite des conditions d'accès spécifiques prévues dans les dispositions mettant en place lesdits traitements, en particulier lorsque lesdites dispositions encadrent explicitement l'accès. La disposition sous examen vise à ce que la Police grand-ducale puisse disposer d'un accès direct, par un système informatique, à ces traitements de données dans la limite des finalités et des modalités des traitements effectués par la Police grand-ducale.
11. À titre d'exemple, l'accès direct au « système électronique central de recherche de données concernant des comptes de paiement et des comptes bancaires identifiés par un numéro IBAN et des coffres-forts tenus par des établissements de crédit au Luxembourg » prévu à l'article 43, paragraphe 2), chiffre 6^o, doit être lu ensemble avec les dispositions de la loi du 25 mars 2020 instituant un système électronique central de recherche de données concernant des comptes IBAN et des coffres-forts. Cette loi prévoit, en vertu de l'article 1^{er} lu ensemble avec l'article 8 de ladite loi que :
- « les agents de police judiciaire et officiers de police judiciaire affectés au Service de police judiciaire, ainsi que les officiers de police judiciaire visés à l'article 10 du Code de procédure pénale et agréés par le directeur général de la Police grand-ducale [...] peuvent, dans la mesure où cela est nécessaire dans l'accomplissement des obligations qui leur incombent en matière de lutte contre le blanchiment et contre le financement du terrorisme, demander à la CSSF, selon la procédure arrêtée par la CSSF et selon les conditions du paragraphe 3, de*

¹⁹⁷ Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7044 portant réforme de l'Inspection générale de la Police, du projet de règlement grand-ducal relatif au fonctionnement de l'Inspection générale de la Police et au projet de loi n° 7045 portant réforme de la Police grand-ducale, Délibération n° 264/2017 du 24 mars 2017.

recevoir sans délai les données visées à l'article 2, paragraphe 1^{er} ».

12. Dès lors, l'article 43, paragraphe 2, point 6°, permet aux agents autorisés de la Police grand-ducale de « *demander à la CSSF [...] de recevoir sans délai les données visées [...]* ».

13. En ce qui concerne l'accès au « *registre des fiducies et des trusts* » visé à l'article 43, paragraphe 2, chiffre 7°, l'article 25 de la loi du 10 juillet 2020 instituant un Registre des fiducies et des trusts, lu ensemble avec l'article 1^{er} de cette loi prévoit, au paragraphe 1^{er}, que « *les officiers de police judiciaire visés à l'article 10 du Code de procédure pénale et agréés par le directeur général de la Police grand-ducale [...] ont accès aux informations visées à l'article 14 inscrites dans le Registre des fiducies et des trusts* » et précise au paragraphe 2 que « *Les modalités de mise en œuvre concernant l'octroi des accès [...] sont fixées par règlement grand-ducal* ». Or, ce règlement grand-ducal n'existe pas en l'état actuel. Quoiqu'il en soit, la loi précitée ne prévoit pas un accès direct et la CNPD s'interroge si les modalités à définir dans le règlement grand-ducal visé puissent effectivement prévoir un tel accès direct sans aller au-delà de l'article 25 de la loi précitée.

14. Concernant l'accès aux registres fonciers, le Règlement grand-ducal du 10 août 2018 portant fixation des conditions et modalités de consultation et de délivrance de la documentation cadastrale, topographique,

cartographique et géodésique gérée par l'administration du cadastre et de la topographie ; et portant fixation du tarif des taxes à percevoir au profit de l'État pour les travaux de bureau et de terrain exécutés par l'Administration du cadastre et de la topographie prévoit en son article 9 que l'Administration du cadastre et de la topographie (ACT) « *accorde des droits d'accès relatifs à la consultation en ligne sous forme de requêtes préétablies d'une partie ou de l'entièreté des registres fonciers [...] aux [...] administrations et services de l'État* ». Il en ressort d'une part un accès indirect, accordé par l'ACT, qui n'est pas équivalent à un accès direct tel que visé dans la disposition sous examen.

15. Concernant l'accès au registre public des bâtiments de plaisance battant pavillon luxembourgeois créé par la loi du 23 septembre 1997 portant réglementation de la navigation de plaisance et portant modification de certaines autres dispositions légales, ladite loi ne prévoit pas explicitement de possibilité d'accès direct, mais semble ouvrir la voie à des demandes de consultation de la part des administrations de l'Etat.

16. Dès lors, la CNPD recommande de préciser la formulation de l'article 43, en ajoutant que l'accès s'effectue « *selon les modalités définies dans les dispositions régissant les traitements de données* » visées dans ladite disposition. À défaut, la disposition sous considération risque de modifier indirectement les lois précitées alors même

6

ANNEXES

qu'un accès direct par d'autres autorités ayant accès aux traitements de données visés n'a pas été voulue initialement par le législateur.

17. Les auteurs expliquent, dans le commentaire des articles, que de leur avis, « *le RGPD n'oblige plus de disposer d'une base légale ou réglementaire spécifique pour l'accès aux données ou pour le transfert de ces données vers une autre administration* ». Cependant, même si ces considérations sortent du cadre strict du présent projet de loi, la CNPD souligne qu'un tel accès direct doit, du point de vue de l'administration en question, être en principe prévu par une disposition légale eu égard notamment à l'article 6, paragraphes 3 et 4, et des considérants, 41, 45 et 50 du RGPD¹⁹⁸. En l'absence d'une telle disposition légale, la CNPD est d'avis que les administrations publiques ne peuvent pas accorder un accès direct à un traitement de données à la Police grand-ducale. Un tel accès est à distinguer d'une transmission au cas par cas sur la base des règles procédurales en place, en particulier en vertu de dispositions du code de procédure pénale.
18. Ainsi, il convient de distinguer l'accès direct de la Police grand-ducale aux données détenues par d'autres administrations d'un accès indirect ou d'une *transmission manuelle* de données par une administration à la Police grand-ducale dans l'exécution des missions de police judiciaire ou de police administrative ou des missions découlant

d'une loi spéciale. À cet égard, la CNPD ne peut pas souscrire à l'analyse proposée de l'article 6, paragraphe 1^{er}, lettre e), du RGPD par les auteurs dans le commentaire des articles.

1.1. Les finalités

19. L'article 43, paragraphe 1, nouveau prévoit que :
- « *Dans l'exercice de leurs missions de police judiciaire et de police administrative ou à des fins administratives, les membres de la Police ayant la qualité d'officier ou d'agent de police judiciaire ou d'officier ou d'agent de police administrative ont accès direct, par un système informatique, aux traitements de données à caractère personnel suivants : [...]* »
20. L'article 43, paragraphe 2, nouveau prévoit (?) également que l'accès direct peut se faire « *dans l'exercice de leurs missions de police judiciaire et de police administrative ou à des fins administratives* ». Il n'y a pas, à cet égard, de différence entre le paragraphe 1^{er} et 2 de la disposition sous examen, si ce n'est que concernant la liste des personnes pouvant avoir accès qui fera l'objet de développements plus loin.
21. Or, la Commission nationale note avec regret que, outre l'accès déjà existant « *dans l'exercice de leurs missions de police judiciaire et de police adminis-*

¹⁹⁸ Pour les critères qu'une telle disposition légale doit remplir, voir notamment BESCH, Marc, « *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 : « *Or, tel que le relève le Conseil d'Etat, dans le respect de l'article 11, paragraphe 3, de la Constitution, qui érige en matière réservée à la loi les exceptions à la garantie par l'État de la protection de la vie privée, les conditions dans lesquelles les données peuvent être traitées à une finalité autre que celle pour laquelle elles ont été collectées doivent faire l'objet d'une loi, du moins quant aux éléments essentiels de la matière.* »

trative »¹⁹⁹, les auteurs proposent que les membres de la Police grand-ducale peuvent accéder aux mêmes bases de données « à des fins administratives », c'est-à-dire une finalité additionnelle aux accès au motif de police administrative, et non autrement définie.

22. Dans l'exposé des motifs, les auteurs du projet de loi expliquent que « [l']adaptation envisagée a pour but d'adapter la liste des fichiers déjà accessibles à la Police et de mieux encadrer leur accès par la Police ». Or, la proposition actuelle vise à étendre les accès plutôt que de les encadrer. Dans le commentaire des articles, les auteurs expliquent cette extension d'accès direct à des « fins administratives » par le fait que :

« Toutefois, la Police est également en charge de missions légales qui ne rentrent ni dans l'une, ni dans l'autre catégorie. C'est par exemple le cas en matière des objets trouvés ou de la police des étrangers. Par ailleurs, certains membres de la Police ont besoin d'un accès à certaines banques de données à des fins purement administratives, par exemple, dans le cadre des ressources humaines ».

23. La CNPD note d'abord que l'accès pour des « fins administratives » semble plus large que « l'exécution de missions à des fins autres que celles visées au paragraphe 1^{er} et prévues par des lois spéciales », visée à l'article 1^{er}, paragraphe 2, lettre a), de la loi du 1^{er} août 2018 relative aux

traitements de données en matière pénale et vise également des traitements qui ne tombent pas sous le champ d'application de la loi précitée du 1^{er} août 2018, mais qui relève du champ d'application du RGPD. En particulier, la CNPD n'est pas convaincue que des traitements de données « dans le cadre des ressources humaines », ne relevant manifestement pas des missions visées par des lois spéciales, puissent justifier un accès direct à toutes les banques de données visées par la disposition sous examen. Dès lors, la CNPD propose de supprimer la mention de l'accès direct à des « fins administratives » aux traitements de données effectuées par d'autres administrations à chaque occurrence dans l'article 43, paragraphes 1^{er} à 4 nouveau.

24. Si le législateur venait à suivre le raisonnement des auteurs du projet de loi, d'autres administrations pourraient revendiquer un accès aux fichiers visés par cette disposition pour des « fins administratives », notamment la gestion des « ressources humaines ». Il semble évident qu'en règle générale, un tel accès direct est disproportionné dans la poursuite desdites finalités et à proscrire.
25. Pour les autres missions de la Police grand-ducale, prévues dans des lois spéciales, il conviendrait d'analyser, par type de mission, à quelle base de données il conviendrait de donner accès. À titre d'illustration en reprenant les exemples proposés par les

¹⁹⁹ Dans son avis précité relatif au projet de loi n° 7045, la CNPD s'est déjà demandé « s'il est justifié que les bases de données auxquelles la Police grand-ducale a accès dans le cadre des missions de police administrative soient identiques à celles auxquelles elle a accès dans le cadre des missions de police judiciaire ».

6

ANNEXES

auteurs dans le commentaire des articles, la CNPD s'interroge sur la nécessité d'accéder, « en matière des objets trouvés », au « fichier relatif aux affiliations des salariés, des indépendants et des employeurs géré par le Centre commun de la sécurité sociale sur base de l'article 413 du Code de la Sécurité sociale » ou au « registre foncier ».

1.2. Le contrôle des accès

26. L'article 43, paragraphe 7, prévoit que

« Nonobstant les droits d'accès prévus aux paragraphes (1) à (4), les données à caractère personnel consultées doivent avoir un lien direct avec les motifs de consultation. Seules les données à caractère personnel strictement nécessaires, dans le respect du principe de proportionnalité, peuvent être consultées. »

27. Il apparaît que le renvoi au « respect du principe de proportionnalité » porte à confusion alors que, dans le contexte du passage sous examen, il convient de comprendre la limitation de l'accès aux données à caractère personnel aux seules personnes autorisées ayant un intérêt légitime à les connaître aux fins de cette opération de traitement (principe défini en anglais sous le terme « need to know/need to do »). Cependant, de manière générale, ledit principe est connu également comme le principe de minimisation des données, c'est-à-dire 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.

28. D'une part, il conviendrait de changer la terminologie employée dans ledit paragraphe pour lever cette confusion, et d'autre part, il revient au responsable de traitement de définir les accès de sorte que l'accès à une information ne peut être attribué que lorsque l'utilisateur a le besoin spécifique de la connaître et/ou de faire des modifications.

29. La CNPD note avec intérêt que les auteurs proposent de scinder la liste de ces bases de données en deux groupes, permettant de définir des accès différents par groupe de bases de données.

30. L'accès du premier groupe, suivant la formulation de l'article 43, paragraphes 1^{er}, peut être attribué aux « membres de la Police ayant la qualité d'officier ou d'agent de police judiciaire ou d'officier ou d'agent de police administrative ». L'accès au deuxième groupe, suivant la formulation de l'article 43, paragraphes 2, peut être attribué aux

« membres de la Police ayant la qualité d'officier de police judiciaire ou d'officier de police administrative [...] s'ils font partie d'une entité de la Police dont les missions justifient cet accès ou figurent sur une liste agréée par le directeur général de la Police après avis du délégué à la protection des données de la Police ».

L'article 43, paragraphe 4 prévoit par ailleurs que

« les membres de la Police ayant la qualité d'agent de police judiciaire ou d'agent de police administrative nommément désignés par le directeur général de la Police grand-ducale, après avis du délégué à la protection des données de la Police, peuvent avoir accès aux fichiers prévus aux paragraphes (2) ».

Les auteurs du projet de loi justifient l'insertion du paragraphe 4 pour « pouvoir attribuer ces mêmes accès aux agents de police judiciaire ». D'abord, il en ressort implicitement que l'accès au premier groupe est attribué, sans distinction de leurs attributions ou tâches concrètes, à tous les membres de la Police visés au paragraphe 1^{er}. Ainsi, les auteurs du projet de loi expliquent que « tous les officiers et agents de police judiciaire dans des fonctions opérationnelles ont besoin de pouvoir accéder pour l'accomplissement de leurs missions ordinaires ». En combinant le paragraphe 2 et le paragraphe 4, il ne ressort pas de distinction claire entre l'attribution des accès au deuxième groupe aux officiers et aux agents de police, en particulier lorsque l'accès n'est pas lié aux missions de l'entité à laquelle le membre de la Police est affecté. Ainsi, la CNPD se demande s'il ne serait pas opportun de préciser le paragraphe 4 en précisant les conditions d'attributions.

31. L'article 43, paragraphe 3 permet d'étendre les accès au premier et au deuxième groupe aux « membres du cadre civil de la Police, nommément désignés par le ministre [...] sur proposition du directeur général de la Police grand-ducale [...] en fonction de leurs attributions spécifiques de support d'un officier ou agent de police judiciaire ou d'un officier ou agent de police administrative ou à des fins administratives ». Sous réserve des commentaires ci-dessous concernant les profils et modalités d'accès ainsi que de son opposition à la référence aux « fins administratives », la CNPD peut s'accommoder de l'extension des accès aux membres du cadre civil tel que proposée dans ce paragraphe.

32. La CNPD regrette cependant que la disposition sous examen reste muette sur les critères de détermination des profils et des modalités d'accès. Comme développé plus haut, de l'avis de la CNPD, l'accès aux traitements de données visés à l'article 43 est subordonné au respect des dispositions législatives et réglementaires spécifiques. Il serait dès lors opportun d'inclure les limitations d'accès prévues dans lesdites dispositions dans les critères de détermination des profils et des modalités d'accès.

33. Dans l'exemple exposé plus haut concernant le système électronique central de recherche de données concernant des comptes de paiement et des comptes bancaires identifiés par un numéro IBAN et

6

ANNEXES

des coffres-forts tenus par des établissements de crédit au Luxembourg, seuls les « *agents de police judiciaire et officiers de police judiciaire affectés au Service de police judiciaire, ainsi que les officiers de police judiciaire visés à l'article 10 du Code de procédure pénale et agréés par le directeur général de la Police grand-ducale* » sont autorisés à bénéficier d'un tel accès direct, sous réserve des considérations exposées précédemment relatives aux modalités d'accès prévus dans les législations afférentes aux différents traitements.

34. L'article 43, paragraphes 6 et 7 reprennent le texte de l'article 43 existant dans les grandes lignes. La disposition ne fournit pas de détails sur ce que le lien direct entre les motifs de la consultation et les données consultées signifie, ni de comment le caractère « *strictement nécessaire* » et proportionnel est vérifié.
35. La Commission nationale propose que les profils et modalités d'accès soient définis en se basant sur l'article 43-1, paragraphe 3.
36. L'article 43, paragraphe 8 nouveau, est une disposition héritée du fonctionnement de l'autorité « *article 17* » instaurée par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, abrogée depuis. Cette disposition exige que la CNPD « *contrôle et surveille le respect des conditions d'accès* » tel que défini à l'article 43 nouveau. Or, deux obser-

vations sont à formuler à cet égard. D'abord, la loi du 1er août 2018 portant organisation de la CNPD prévoit que la Commission nationale « *contrôle l'application des dispositions et des mesures d'exécution et veille au respect* » de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale. Ces missions et pouvoirs générales englobent la surveillance et le contrôle des accès concernant tous les traitements de données visées en matière pénale, y compris ceux visés par la disposition sous examen. Ensuite, la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale constitue un changement de paradigme en matière de responsabilisation des responsables de traitement, notamment visé par l'article 3, paragraphe 4, et de l'article 18 de ladite loi. Ainsi, en application notamment de l'article 24 de ladite loi, il revient au responsable de traitement de définir les profils et modalités d'accès et procéder à des vérifications régulières des logues à des fins, notamment, « *d'autocontrôle [et] de garantie de l'intégrité et de la sécurité des données à caractère personnel* ». A cet égard, la CNPD souligne l'importance d'effectuer proactivement des contrôles en interne, notamment en lien avec les mesures et procédures à mettre en place pour tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement conformément à l'article 28 de ladite loi. Ainsi, la CNPD s'interroge sur la plus-value du paragraphe 8 sous examen, alors que ce type de

contrôle et de surveillance est inclut dans ses missions générales et revient en premier lieu au responsable de traitement, et se demande s'il ne conviendrait pas de supprimer cette disposition.

2. La base légale des fichiers de la Police grand-ducale

37. La Commission nationale note que la Police grand-ducale est appelée à collecter et exploiter structurellement et systématiquement une quantité importante de données à caractère personnel. Nul aucun doute, ces traitements de données sont inhérents à ses missions répressives et sont inévitables pour une autorité publique chargée de l'exercice de la puissance publique en matière pénale et en matière de sécurité nationale.
38. Or, la CNPD rappelle que les traitements de données effectués par la Police grand-ducale dans l'exercice de ses missions de Police administrative et de Police judiciaire constituent une ingérence dans le droit au respect de la vie privée et le droit à la protection des données. Le même constat peut être dressé, en principe, pour les traitements de données effectués dans l'exercice des missions découlant de lois spéciales. Il est constant que toute ingérence dans les libertés fondamentales doit être prévue par une disposition légale accessible et prévisible. Au vue de l'impact potentiel sur la vie des personnes concernées, il est justifié que les dispositions qui encadrent les traitements
- de données de la Police soient à la fois détaillées et contraignantes. Il s'agit de renforcer l'état de droit et le fonctionnement de notre société démocratique en offrant une meilleure sécurité juridique et une confiance accrue dans le fonctionnement des autorités répressives.
39. Les actes, rapports et procès-verbaux établies par les agents de la Police grand-ducale s'inscrivent dans la mise en œuvre du Code pénal, du Code de procédure pénale et des dispositions conférant des missions à la Police grand-ducale découlant de lois spéciales, y compris la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, qui constituent une base légale suffisante pour la collecte de données à caractère personnel dans l'exécution de ces missions essentielles de la Police grand-ducale.
40. Néanmoins, la mise en relation de données personnelles collectées dans des procédures pénales distinctes ou en application de différentes missions de la Police et leur exploitation dans des fichiers transversaux constitue généralement des traitements de données distincts. La plupart de ces traitements de données subséquents constituent donc une ingérence dans la vie privée des citoyens additionnelle à l'ingérence prévues aux dispositions précitées encadrant et définissant les missions de la Police.
41. Dans l'exposé des motifs, les auteurs expliquent que les dispositions en matière

6

ANNEXES

de fichiers particuliers contenues dans le présent projet de loi « *s'inspire[nt] partiellement de la législation belge, et notamment de la loi du 5 août 1992 sur la fonction de police* ». Or, la Commission nationale note que la législation belge prévoit expressément un certain nombre de banques de données régulièrement utilisées et font une distinction plus nette entre les missions de police administrative et de police judiciaire. La CNPD note également que la législation belge prévoit, a minima, l'adoption et la publication de « *directives contraignantes* » et de « *directives générales et contraignantes* » par le ou les Ministres de tutelle. La CNPD note également que la création de « *fichiers particuliers* » au sens de la loi belge est subordonnée à l'existence de « *circonstances spécifiques* » et de « *besoins particuliers* » limitativement définies.

42. La Commission nationale souligne aussi qu'en France, depuis 2018, l'ensemble des fichiers « *mis à la disposition des forces de sécurité* » est encadré chaque fois par une disposition légale ou réglementaire spécifique²⁰⁰.

43. Toutefois, la CNPD comprend également que le fonctionnement de la Police grand-ducale et sa relation avec les autorités judiciaires ne sont pas en tous points identiques et ne sont pas toujours comparables à ses homologues français et belges dans leurs ordres juridiques respectifs, même si, bien-entendu, les

dispositions pénales luxembourgeoises s'inspirent tantôt de l'un, tantôt de l'autre ordre juridique.

44. Dès lors, même si la législation belge ou française peut inspirer le législateur, il convient de prendre en compte les spécificités du cadre légal et des institutions luxembourgeoises. Ainsi, il est primordial que la loi luxembourgeoise satisfasse aux exigences propres à l'ordre juridique luxembourgeois et des engagements européens et internationaux du Grand-Duché de Luxembourg.

45. Ainsi, pour se conformer aux exigences de l'article 11, paragraphe 3, lu à la lumière de l'article 32, paragraphe 3, de la Constitution, de l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme, de l'article 52, paragraphes 1 et 2, de la Charte des droits fondamentaux de l'Union européenne et de la jurisprudence s'y référant, ces traitements de données nécessitent en principe un encadrement législatif distinct. La CNPD rappelle qu'une ingérence dans le droit au respect de la vie privée ou dans le droit à la protection des données 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 ;

²⁰⁰ Assemblée nationale française, Rapport d'information déposé en application de l'article 145 du règlement, par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur les fichiers mis à la disposition des forces de sécurité, n° 1335, 17 octobre 2018.
Voir : https://www.assemblee-nationale.fr/dyn/15/dossiers/alt/fichiers_disposition_forces_securite_rap-info.

- 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.
46. Or, il y a un consensus qu'une grande partie des fichiers existants de la Police grand-ducale, et avant tout le fichier central, ne bénéficient pas, à ce jour, de dispositions législatives ou réglementaires propres mais n'est encadrée que par la seule loi-cadre, la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale.
47. Le fichier central est un outil de travail essentiel qui permet de regrouper, dans une application unique, tous les traitements de données relatives aux actes, rapports et procès-verbaux établis dans l'exécution des missions de police judiciaire, de police administrative et de « *toute autre mission dont la Police est investie* ».
48. À cet égard, la Commission nationale salue que le projet de loi prévoit de doter le fichier central de la Police grand-ducale d'une base légale spécifique. Elle note que le projet de loi prévoit des dispositions concernant le fonctionnement des fichiers exploités par la Police grand-ducale, par le biais de l'article 43-2 nouveau, qui définit les modalités des traitements de données sous-jacents à ce fichier.
49. La Commission nationale note également avec intérêt que l'article 43-1 nouveau

créé un cadre commun applicable à « *tous les fichiers de la Police dans le cadre des missions légales dont elle est investie* », comme le précisent les auteurs du projet de loi dans le commentaire des articles, à moins que des dispositions légales spécifiques prévoient d'autres règles. De plus, ni l'exposé des motifs, ni le commentaire des articles comportent une liste exhaustive des fichiers existants pouvant être visés par les nouvelles dispositions. Bien entendu, en tant qu'autorité de contrôle, la CNPD n'ignore pas quels traitements de données sont effectués par la Police grand-ducale qui sont susceptibles d'être visés par cette disposition. De plus, le gouvernement a fourni des indications sur lesdits traitements dans les réponses aux questions parlementaires concernant les fichiers mis en œuvre par la Police. Par exemple, la réponse datée du 2 août 2019 du Ministre ayant la sécurité intérieure dans ses attributions à une question parlementaire fait état de 53 traitements de données distincts, dont certains sont encadrés par une disposition législative spécifique²⁰¹. Ladite réponse fait également référence à des traitements de données fondés sur des instruments juridiques internationaux et européens. À titre d'illustration, parmi les traitements de données potentiellement visés par la disposition sous examen figurent les traitements de vidéosurveillance « *VISUPOL* »²⁰², la gestion des empreintes digitales, l'« *application PIC* »²⁰³ et le « *fichier stupéfiant* »²⁰⁴. Il est regrettable que les

²⁰¹ Voir question parlementaire n° 906 du 17 juillet 2019 des honorables Députés Laurent MOSAR et Gilles ROTH.

²⁰² À ce sujet, voir le projet de loi n° 7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, ainsi que les avis y relatifs.

²⁰³ Traitement des images et de données relatives à des personnes, voir notamment réponse à la question.

²⁰⁴ QP 1190 Fichier en matière de stupéfiants auprès de la Police grand-ducale.

6

ANNEXES

auteurs n'aient pas fait, a minima, preuve de transparence concernant les fichiers visés à ce jour par cette disposition. Or, dans un souci d'accessibilité et de prévisibilité de la loi, la Commission nationale recommande dès lors, d'identifier les traitements de données mis en œuvre par la Police susceptibles d'être visés par la disposition sous examen, en particulier les traitements de données mis en œuvre en vertu de dispositions légales spécifiques et, tel que détaillé plus loin d'encadrer le cas échéant les fichiers particuliers par les instruments juridiques adéquats.

50. Suivant l'article 43-1, paragraphe 1, la disposition s'applique à tous les fichiers gérés par la Police, « sans préjudice de dispositions légales spécifiques ». Sans tendre vers l'exhaustivité, la CNPD a identifié au moins les dispositions légales spécifiques suivantes :

- Règlement grand-ducal modifié du 21 décembre 2004 portant autorisation de la création d'un fichier des personnes ayant subi un avertissement taxé en matière de circulation routière (« Fichier AT »);
- Règlement grand-ducal du 6 mai 2005 fixant les modalités d'installation et d'exploitation de systèmes d'alarmes reliés au Centre d'Intervention National de la Police ;
- Loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale (« Fichier ADN »);

- Loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement et le Règlement grand-ducal du 5 août 2015 relatif aux fiches à tenir par les logeurs exploitant un service d'hébergement touristique ;
- Règlement grand-ducal modifié 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 automatisés (« Traitement CSA »);
- Fichier central, tel que visé par le présent projet de loi par le biais de l'article 43-2 nouveau ;
- Les systèmes de vidéosurveillance « VISUPOL », lorsque le projet de loi n° 7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale aura été adopté par la Chambre de Députés.

51. La Commission nationale note également que le Code de procédure pénale (CPP) contient un certain nombre de dispositions spécifiques concernant certains traitements de données effectués par la Police, comme par exemple les « mesures spéciales de surveillance »²⁰⁵ ou les dispositions visant la collecte d'empreintes digitales et de photographies²⁰⁶.

52. En application de la législation européenne et d'engagements internationaux, la Police grand-ducale a accès et contribue à des traitements de données transfrontaliers,

²⁰⁵ Ces mesures peuvent être ordonné par le juge d'instruction et visent l'utilisation de moyens techniques de surveillance et de contrôle de toutes les formes de communication, au moyen de (1) de la surveillance et du contrôle des télécommunications ainsi que de la correspondance postale (2) de la sonorisation et de la fixation d'images de certains lieux ou véhicules et (3) de la captation de données informatiques. Voir les articles 88-1 à 88-4 CPP.

²⁰⁶ Voir notamment articles 33, paragraphe 9, et 51-2 CPP.

par exemple au système d'information Schengen de deuxième génération (SIS II), aux traitements de données mis en œuvre par Europol et Interpol²⁰⁷ ainsi qu'aux traitements de données opérés par le Centre de coopération policière et douanière²⁰⁸.

53. Le projet de loi ne prévoit pas de dispositions législatives ou réglementaires pour la création de fichiers autres que le fichier central. Or, la Commission nationale note avec regret que le projet ne contient ni des règles procédurales pour la création de fichiers « particuliers » ni d'exigences de recourir à une disposition légale ou réglementaire. Ainsi, l'article 43-1 prévoit un cadre relatif aux fichiers particuliers, mais ne précise pas sur quelle base ou quelle décision de tels fichiers « particuliers » puissent être mis en place. Il est ainsi laissé à la libre appréciation de la Police grand-ducale de procéder à la création d'un tel fichier. La CNPD ne considère pas que cette solution satisfasse aux exigences légales décrites plus haut.

54. La CNPD propose de distinguer deux catégories de fichiers particuliers :

- Les fichiers particuliers existant pour combler des limitations techniques d'un fichier existant fondé sur une disposition légale, comme le fichier central ou un autre fichier particulier mis en œuvre par la Police. Ce type de fichier particulier s'inscrirait ainsi dans les modalités des traitements de données du fichier « principal » et ne

nécessiterait pas de disposition légale ou réglementaire spécifique. En effet, il pourrait être considéré que certains fichiers « techniques » constituent une prolongation du fichier central lorsque les données visées par ces fichiers ne peuvent pas figurer, pour des raisons techniques, dans le fichier central. Tel est d'ailleurs la logique retenue à l'article 43-2, paragraphe 18, alinéa 2, pour la conservation, après l'écoulement du délai de conservation prévu pour la partie active du fichier central, des « informations et données à caractère personnel [...] dans un format qui ne peut pas être géré par le fichier central ». En effet, l'alinéa en question prévoit la création d'une partie passive dans le fichier particulier concerné suivant les mêmes dispositions relatives aux durées de conservation que dans la partie passive du fichier central ;

- Les fichiers particuliers
 - qui traitent des catégories particulières de données ,
 - qui sont conçus pour effectuer des opérations de traitement de données « intrusives », du type profilage, de comparaison et de suivi de personnes physiques ou
 - qui nécessitent, par la nature des données stockées (comme par exemple des preuves et traces), de conserver les informations pour des durées de conservation plus étendues.

Ces types de fichiers particuliers devraient être encadrés par une disposition légale.

²⁰⁷ Voir également, à titre d'illustration, le système d'information d'Europol (Europol Information System, EIS) et l'application de réseau d'échange d'informations sécurisées d'Europol (Secure Information Exchange Network Application, SIENA), les bases de données mises en commun au niveau de l'Organisation internationale de police criminelle (Interpol).

²⁰⁸ Accord entre le Gouvernement du Grand-Duché de Luxembourg, le Gouvernement du Royaume de Belgique, le Gouvernement de la République fédérale d'Allemagne et le Gouvernement de la République française, concernant la mise en place et l'exploitation d'un centre commun de coopération policière et douanière dans la zone frontalière commune, signé à Luxembourg, le 24 octobre 2008 et entré en vigueur le 1^{er} décembre 2014.

6

ANNEXES

55. Il est entendu que, s'il est nécessaire de créer un fichier particulier dans l'exécution d'une mission découlant d'une loi spéciale ou dans la mise en œuvre d'une disposition légale, cette loi spéciale ou disposition peut en constituer la base légale et l'article 43-1 pour encadrer ces fichiers.

3. Les finalités du fichier central et des fichiers particuliers

56. Conformément à l'article 3, paragraphe 1^{er}, lettre b), les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités ». À cet égard, au-delà, d'après les termes des auteurs du projet, de la fonction générale du fichier central « de centraliser les données à caractère personnel et informations relatives aux personnes concernées traitées dans le cadre de l'exécution d'une mission légale » telle qu'identifiée par l'article 43-2, paragraphe 1^{er}, la CNPD se réjouit que le projet de loi définisse les finalités au paragraphe 2 :

« Les données à caractère personnel et informations sont traitées dans le fichier central pour les finalités suivantes :

1° la vérification des antécédents d'une personne dans le cadre d'une mission de police judiciaire, de police administrative ou dans le cadre d'une autre mission légale de la Police ;

2° l'appui aux enquêtes judiciaires par le biais d'analyses criminelles opérationnelles à la demande d'une autorité judiciaire ;

3° l'appui à la définition et à la réalisation de la politique de sécurité intérieure par le biais d'analyses criminelles stratégiques ;

4° l'exploitation des informations à des fins de recherches statistiques ;

5° l'identification des membres de la Police en charge du dossier. »

57. La Commission nationale note que les finalités mélangent les finalités liées aux trois groupes de missions.

58. Il ressort du projet de loi que les données peuvent être collectées et utilisées pour des finalités liées à la coopération policière internationale et à l'entraide judiciaire internationale, à des rapports aux autorités judiciaires concernant des mineurs, pour des rapports adressés aux autorités judiciaires et aux autorités administratives. En particulier en matière de missions de police administrative et de « toute autre mission dont la Police est investie par la loi », elle suggère que la disposition sous considération soit davantage détaillée.

59. L'article 43-1 ne définit pas de finalités pour les fichiers « particuliers ». La CNPD se pose la question si ces fichiers peuvent poursuivre des finalités différentes de celles du fichier central. Elle renvoie à sa proposition

concernant la distinction à faire entre fichiers particuliers. Les finalités des fichiers « *techniques* » seraient identiques aux finalités du fichier « *principal* » auxquels ces fichiers se rapportent. Les dispositions légales spécifiques devront définir les finalités des autres fichiers. À titre d'exemple, un fichier particulier ayant comme fonction de comparer de nouvelles preuves et traces par rapport au contenu d'une base de données existante poursuit des finalités dépassant les finalités définies pour le fichier central et permet d'effectuer des opérations de traitements de données spécifiques de comparaison et de recherche semi-automatisés. De l'avis de la CNPD, il serait préférable que les finalités de ce type de fichier (en particulier les fichiers « *biométriques* », visant des empreintes digitales, génétiques et de reconnaissance faciale) soient encadrées par une disposition légale.

60. La CNPD peut se rallier aux deux finalités pouvant justifier l'accès aux données contenues dans la partie passive du fichier central et de la partie passive des fichiers particuliers, réservées aux données relevant des missions de police judiciaire, telles que définies à l'article 43-2, paragraphe 19 alinéa 1er. Elle note que ces données peuvent aussi faire l'objet d'une retransmission dans la partie active du fichier concernée dans les cas de figure visés à l'article 43-2, paragraphe 16.
61. La Commission nationale estime que, dans le cas visé à l'article 43-2, paragraphe 18,

alinéa 2, en ce qui concerne les fichiers particuliers ne disposant pas de partie active, que les accès devront être limités de la même façon aux finalités visées plus haut, tout en exprimant ses réserves quant à l'absence d'une telle partie passive.

4. Les données traitées dans les fichiers particuliers et dans le fichier central

62. Conformément à l'article 5 de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale, l'article 43-2, paragraphes 3 et 4, définit les catégories de personnes dont les données sont traitées sous l'angle des trois catégories de missions confiées à la Police et définit quelles catégories de personnes saisies à des fins de police judiciaire peuvent également être consultées dans l'exercice d'autres missions. Ainsi, au titre de l'article 43-2, paragraphe 5, les données relatives à des victimes, des témoins ou des personnes visées par des données « *douces* » ne peuvent pas être consultées à des fins de police administrative et des autres missions légales de la Police. Dans l'exécution des missions de police administrative, les données « *douces* » ne sont pas accessibles. La CNPD accueille favorablement que l'accès à des données de certaines catégories de personnes soit limité aux missions de police judiciaire et ne peuvent dès lors pas être consultés à des fins des missions de police administrative ou des autres missions légales de la

Police. La Commission nationale peut en général souscrire à la solution proposée auxdits paragraphes 3 à 5. Néanmoins, les catégories de données définies dans les instruments européens, notamment en matière de SIS II et d'Europol, peuvent être pris en considération pour affiner les définitions desdites catégories au niveau national, dans un souci de transparence et de cohérence.

63. Il semble que les fichiers particuliers puissent contenir les mêmes catégories de données et opérer les mêmes distinctions en matière de personnes concernées. Or, il conviendrait de déterminer ces distinctions dans l'instrument juridique servant de base légale pour ces fichiers.

4.1. Les catégories particulières de données

64. L'article 9 de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale relatif au traitement de données des catégories particulières de données, prévoit que :

« Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des don-

nées concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont autorisés uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :

- a) lorsqu'ils sont autorisés par le droit de l'Union européenne ou en application de la présente loi ou d'une autre disposition du droit luxembourgeois ;*
- b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique, ou*
- c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée. »*

65. Il semble qu'en particulier les fichiers destinés à contenir des traces et preuves puissent viser des catégories supplémentaires de données, y compris des catégories particulières de données. La Commission nationale note que, en ce qui concerne le fichier central, les « *signes corporels inaltérables permettant d'identifier la personne, y compris photographies et, le cas échéant, les empreintes digitales* » visées à l'article 43-2, paragraphe 7, alinéa 2, chiffre 10, peuvent, suivant les opérations de traitement de données effectuées, relever des données biométriques.

66. La CNPD note avec intérêt que l'article 43-1, paragraphe 2, permet à la Police de traiter les catégories particulières de données et exige que, d'une part, ces données aient

« toujours un rapport avec d'autres données relatives à la personne concernée » et que d'autres part ces données soient « pertinentes et essentielles » à :

1. « à l'aide de l'identification d'une personne »;
2. « pour comprendre le contexte décrit dans un rapport ou procès-verbal établi par la Police »;
3. « pour apprécier correctement les faits qui peuvent donner lieu à une infraction pénale ou à une mesure de police administrative au sens de la section 1^{ère} du chapitre 2 de la présente loi ou en vertu d'une autre mission dont la Police est investie par la loi ».

67. La CNPD relève positivement qu'une telle base légale soit créée au sens de l'article 9, lettre a), de la loi du 1^{er} août 2018 précitée et comprend que celle-ci s'applique indifféremment aux fichiers particuliers et au fichier central.

68. Néanmoins, elle s'interroge sur la possibilité, telle qu'esquissée dans le commentaire des articles, d'effectuer des recherches sur ce type de données. Elle suggère de prévoir des garanties supplémentaires pour contrôler ce type de recherche. De plus, elle se demande s'il ne conviendrait pas de prévoir la possibilité d'occulter ce type de données, c'est-à-dire de pseudonymiser ces données, lors des recherches sur la personne concernée à des fins autres que les missions de police judiciaire.

69. Dans le commentaire des articles, les auteurs estiment que « la Police doit être en mesure d'exploiter ce type de données à des fins statistiques, auquel cas les données en question sont anonymisées ». Or, dès lors qu'une réidentification de la personne concernée reste possible, il s'agit plutôt d'une pseudonymisation de données. Il serait préférable d'inclure l'établissement de statistiques dans la définition des finalités, en y précisant que cette opération de traitement de données devrait se baser uniquement sur des données pseudonymisées.

70. La CNPD tient à relever que trois fichiers existants sont structurellement concernés par cette disposition, à savoir le fichier « PIC » (c'est-à-dire englobant les photos de personnes à des fins d'identification), le fichier relatif aux empreintes digitales et le fichier relatif aux empreintes génétiques. La CNPD suggère de légiférer en cet endroit pour inclure une base légale solide assortie des garanties appropriées pour les traitements de photos (actuellement : comme empreintes digitales : Code de procédure pénale, article 33, paragraphe 9 et article 45) recourant à des techniques d'identification faciale, de plus en plus répandues et performantes, c'est-à-dire à des « données biométriques aux fins d'identifier une personne physique de manière unique ». Parmi les garanties appropriées encadrant un tel recours à des techniques d'identification biométrique, une limitation d'utilisation à des fins de

6

ANNEXES

police judiciaire dans le contexte de délits et de crimes pourrait être envisagée.

71. Alors que le traitement de données génétiques bénéficie d'ores et déjà d'un encadrement législatif spécifique à travers la loi modifiée du 25 août 2006 relative aux empreintes génétiques en matière pénale, la CNPD se demande s'il ne serait pas opportun de prévoir également une base légale générale pour les empreintes digitales, dont le traitement est actuellement déjà prévu par des dispositions du Code de procédure pénale (article 33, paragraphe 9, article 45), permettant par la même occasion de combler les éventuelles faiblesses dans ladite loi modifiée du 25 août 2006.

72. La CNPD estime qu'il conviendrait de renforcer les garanties appropriées, par exemple en s'inspirant davantage de la loi belge, en particulier de l'article 44/2, paragraphe 2. D'une part, cette disposition encadre davantage les finalités pour lesquelles ce type de données peuvent être traitées et d'autre part prévoit des règles strictes pour ce qui est de leur utilisation, de leur accès et des règles de sécurité supplémentaires à mettre en place par le responsable de traitement.

4.2. Les données dites « douces »

73. L'article 43-2, paragraphe 4, point 10°, permet à la Police grand-ducale de traiter, dans le fichier central et à des fins de police judiciaire, des données dites

« douces » relatives à trois catégories de personnes :

- « les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles sont sur le point de commettre une infraction pénale » ;
- « les contacts ou associés qui sont suspectés d'avoir l'intention de participer à ces infractions ou d'en avoir connaissance » ;
- « les personnes qui peuvent fournir des informations sur ces infractions pénales ».

74. L'inscription de ce type de données dans le fichier central, que les auteurs définissent dans le commentaire des articles comme des données « qui ne peuvent pas encore être rattachées à une infraction pénale suffisamment qualifiée afin que l'article 12 du Code de procédure pénale devienne applicable », est particulièrement encadrée dans le projet de loi sous considération.

75. D'abord, la CNPD relève positivement que seul un nombre limité d'agents peuvent saisir ce type d'informations, conformément à l'article 43-2, paragraphe 4, alinéa 2, à savoir « les officiers de police judiciaire du Service de police judiciaire dans les matières qui relèvent des attributions de la section à laquelle ils sont affectés ».

76. Ensuite, la CNPD note avec intérêt que l'inscription dans le fichier central est subordonnée à ce que « la fiabilité de la source

- et de l'information est évaluée suivant un code d'évaluation préalablement défini qui tient compte de la pertinence de la source et de l'information fournie dans le contexte de l'évolution de la criminalité et des phénomènes criminels pertinents ». Néanmoins, à cet égard, la CNPD regrette que le projet de loi et le commentaire des articles restent muets sur le « code d'évaluation préalablement défini ». Il serait possible de s'inspirer de la grille d'évaluation prévue à l'article 29 du Règlement (UE) 2016/794 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol)²⁰⁹ relatif à l'évaluation de la fiabilité de la source et de l'exactitude des informations.
77. Finalement, la CNPD peut souscrire à la garantie protégeant les intérêts des mineurs en ce que l'inscription de données douces relatives à des mineurs dépend de « l'accord du procureur général d'Etat ou du membre de son parquet désigné à cet effet ».
78. Concernant les accès, les règles se dégagent de l'article 43-2, paragraphe 5, alinéas 2 à 4.
79. Au titre de l'alinéa 3, les « *officiers et les agents de police judiciaire du Service de police judiciaire* » ont accès à la donnée douce pour les recherches à des fins de police judiciaire et que cet accès peut être limité à « une ou plusieurs sections du Service de police judiciaire ».
80. La CNPD peut souscrire à la solution retenue à l'alinéa 2, à savoir qu'une recherche sur une personne concernée par un agent non affecté au Service de police judiciaire ne lui donne pas accès à l'information, mais donne lieu à un « *avertissement auprès des officiers de police judiciaire en charge de l'information* », leur laissant le soin « *d'évaluer l'utilité de prendre contact avec l'agent consultant* ».
81. Finalement, l'alinéa 4 ménage, pour les « agents en charge de l'information », la possibilité de rendre accessibles les données douces relatives aux « personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles sont sur le point de commettre une infraction pénale », suivant les mêmes règles qu'applicables aux données relatives à « les personnes suspectées d'avoir participé à une infraction pénale ». Or, alors que le commentaire des articles reste muet sur ce point, la CNPD s'interroge sur les critères pouvant justifier un tel accès et se demande si l'« accès direct » inclut l'accès à des fins de police administrative ou à des fins d'autres missions de la Police.
82. Les durées de conservation des données douces ont été adaptées à leur spécificité, en limitant la durée de conservation dans la partie active à un an, pouvant être reconduit d'une année supplémentaire, et à 3 ans dans la partie passive du fichier central.

²⁰⁹ Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, Journal Officiel de l'Union européenne, L 135, 24 mai 2016, pp. 53–114.

6

ANNEXES

83. Ainsi, dans l'ensemble, la CNPD accueille favorablement la solution proposée pour le traitement des données dites « douces », nécessaire à l'accomplissement de tâches liées à la prévention et la détection d'infractions pénales tout en prenant en compte qu'au moment de la collecte de l'information, aucune infraction pénale n'ait encore été commise par la personne concernée. Elle estime en effet que l'équilibre entre les besoins opérationnels à des fins de missions de police judiciaire et les droits des personnes concernées est satisfaisant au regard du principe de proportionnalité.

4.3. Données relatives à des mineurs

84. Le considérant 50 de la Directive 2016/680 prévoit que « les mesures prises par le responsable du traitement devraient comprendre rétablissement et la mise en œuvre de garanties spécifiques destinées au traitement de données à caractère personnel relatives aux personnes physiques vulnérables, telles que les enfants ». Dans son avis sur le fichier central, la Commission nationale avait estimé que « [l]e traitement mis en œuvre par la Police à travers ledit fichier doit également conférer un degré de protection particulier à l'égard des personnes physiques mineures ». À cet égard, elle se réjouit que, tel qu'il découle de l'article 43-1, paragraphe 3, chiffre 6, l'accès aux données relatives à des mineurs fait partie des critères pour définir les droits d'accès et que l'accès à ces données soit en principe réservé aux

« membres de la section 'protection de la jeunesse' au sein du Service de police judiciaire » et, tel que le décrivent les auteurs du projet, « les officiers et agents de police judiciaire qui sont effectivement chargés d'une enquête par rapport au mineur concerné ».

5. Le contrôle des accès aux fichiers particuliers et au fichier central

85. L'accès à la partie active du fichier central est encadrée par quatre niveaux d'accès qui découlent de l'article 43-2, paragraphe 7 :

- Détermination si une personne figure au fichier central ;
- Visionnage des informations et données à caractère personnel principales (définies à l'article 43-2, paragraphe 7, alinéa 2) relatives à la personne ;
- Visionnage d'un résumé sommaire des faits dans lesquels la personne est impliquée ;
- Accès aux procès-verbaux et rapports dont la personne fait l'objet.

86. Ces accès sont accordés « [d]ans le respect des règles d'accès déterminées en vertu de l'article 43-1, paragraphe (3) » et en fonction « des motifs de la consultation ».

87. L'article 43-2, paragraphe 7, permet également d'accorder ces droits d'accès aux « membres du personnel civil nommé désignés par le responsable du traitement ». Contrairement aux modifications

- introduites à l'article 43 nouveau, la CNPD soulève que cette disposition ne restreint pas explicitement cet accès « *en fonction de leurs attributions spécifiques de support d'un officier ou agent de police judiciaire ou d'un officier ou agent de police administrative* ».
88. Il ressort de l'article 43-2, paragraphe 5, des limitations générales concernant les consultations pour un motif, d'une part, de police administrative et à des fins d'autres missions légales, et d'autre part, de police des étrangers. De plus, l'accès aux données « *douces* » est également encadré.
89. Il ressort du commentaire des articles relatif à l'article 43-2, paragraphe 7, que le « *visionnage des informations et données à caractère personnel principales* » est accordée aux « *agents du terrain* ». La CNPD prend bonne note que, d'après le commentaire des articles, « *le détail des procès-verbaux et rapports dont la personne a fait l'objet ne sont accessibles qu'en fonction des droits d'accès et des motifs de la consultation, lesquels sont plus stricts que ceux pour un accès aux informations principales* ».
90. Alors que l'article 43-2, paragraphe 7, alinéa 1^{er}, in fine, conditionne uniquement l'accès aux procès-verbaux et rapports aux « *motifs de la consultation* », la Commission nationale regrette que le projet de loi et le commentaire des articles restent muets sur ces motifs de la consultation.
91. Elle prend bonne note des accès accordés aux officiers de police judiciaire de l'Administration des douanes et accises « *nommément désignés* » et l'Inspecteur général de la Police, à l'Inspecteur général adjoint de la Police et aux membres du cadre policier de l'Inspection générale de la Police, conformément à l'article 43-2, paragraphe 6. L'article 5 du projet de loi supprime l'accès direct du Service de renseignement (SRE) à « *la partie 'recherche' de la banque de données nominatives de police générale* » au motif, d'après le commentaire des articles, qu'il s'agit d'une « *banque de données que le présent projet de loi vise à supprimer* ». La CNPD se demande si le SRE aura accès, par un autre moyen, aux données du fichier central à créer en vertu de la présente loi, et, dans la négative, quel raisonnement a été suivi pour ne pas prévoir un tel accès.
92. En l'absence de dispositions légales spécifiques, l'accès aux fichiers particuliers est déterminé par l'article 43-1, paragraphe 3. La Commission nationale se félicite que cette disposition détaille, pour le fichier central et les fichiers particuliers, les « *profils et des modalités d'accès et de traitement de données à caractère personnel* » et se montre, dans l'ensemble, satisfait de ces critères basés, selon le commentaire des articles, sur « *les principes du need to know et need to do* » et « *attribués en fonction de l'emploi effectif qu'occupe le membre de la Police* ». L'accès aux données relatives

6

ANNEXES

aux mineurs font l'objet de conditions d'accès particulières. Toutefois, elle regrette que l'accès aux catégories particulières de données ne soit pas autrement encadré.

93. Dans son avis sur le fichier central, la Commission nationale avait constaté que « [s]elon les informations de la Police, l'accès au fichier central est accordé d'office à chaque nouvel agent ou officier de police judiciaire, étant donné qu'il pourra être amené à travailler avec cet outil », ce qui signifie en pratique qu'« un total de 1840 personnes disposaient des accès logiques nécessaires afin de pouvoir utiliser le système pour effectuer des recherches respectivement consulter des dossiers ». Or, elle avait conclu qu'« un accès permanent au fichier central pour quasiment 2'000 policiers, même en absence de cas d'abus démontré, comparé à la réelle nécessité de consultation sur le terrain, doit être considérée comme inadéquat. Même en l'absence d'une refonte approfondie du mécanisme d'accès, la CNPD estime que la Police aurait pu et dû implémenter des mesures comme la mise en place de revues de logues pour détecter d'éventuels accès douteux pour mitiger le risque d'abus et assurer la protection des données des citoyens ».
94. Dès lors, elle s'attendra à ce que les critères définis à l'article 43-1, paragraphe 3, résulte en pratique dans une revue des droits d'accès, accompagné de la mise en place de revues de logues régulières. Comme déjà évoqué plus haut, l'article 24 de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale exige du responsable de traitement de définir les profils et modalités d'accès et procéder à des vérifications régulières des logues à des fins, notamment « *d'autocontrôle [et] de garantie de l'intégrité et de la sécurité des données à caractère personnel* ». Il en ressort que le responsable de traitement est censée procéder à des revues de logues régulières et proactives, notamment en lien avec les mesures et procédures à mettre en place pour tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement conformément à l'article 28 de ladite loi.
95. L'article 24, paragraphe 1^{er}, de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale prévoit
- « *Des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé : la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel.* »

96. Il découle incontestablement des articles 18 et 28 de la loi 1^{er} août 2018 relative aux traitements de données en matière pénale que la revue des logues fait également partie des mesures de sécurité à mettre en place par le responsable de traitement. Il découle également de l'article 28 qu'il convient d'adopter les « *mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel* » et donc, lorsque c'est pertinent, de prendre en compte la nature des données, notamment de catégories particulières de données, de données relatives à des mineurs et des données « douces », dans la définition des revues régulières des logues.

97. Dans l'avis relatif au fichier central, la CNPD avait aussi relevé que

« vu que la pratique courante consiste à ce que les policiers sur le terrain n'accèdent pas directement au fichier, mais font plutôt appel à des policiers au niveau du RIFO, l'identification de la personne qui a in fine consulté le système ne peut pas être retracé de manière systématique avec des efforts raisonnables. »

98. À cet égard, il y a lieu de saluer la clarification apportée par l'article 43-1, paragraphe 3, alinéa 2, que « [dans] le cas d'une demande de consultation d'un fichier par une

personne autre que celle qui l'effectue, les journaux du fichier font mention de l'identité de la personne à l'origine de la demande et du motif de cette demande. »

99. L'article 43-1, paragraphe 3, chiffre 4^o, dispose que la

« Police détermine les profils et des modalités d'accès et de traitement de données à caractère personnel sur la base [...] du motif d'accès. Si le motif d'accès ne découle pas incontestablement de l'affectation de l'agent au sein d'un service ou d'une unité de la Police, le motif d'accès doit indiquer la raison précise de la consultation. La Police détermine des motifs d'accès spécifiques selon le type de mission légale de la Police dans le cadre de laquelle un traitement de données est requis ».

100. La CNPD comprend que les auteurs du projet de loi suggèrent que le motif d'une consultation pourrait découler « *incontestablement de l'affectation de l'agent au sein d'un service ou d'une unité de la Police* ». Le commentaire des articles n'élabore pas en quoi l'information de l'affectation d'un agent pourrait donner suffisamment d'information contextuelle afin de retracer la licéité de ladite consultation. La seule identification de l'agent, y compris avec son affectation, rendrait une vérification des logues fastidieuse et peu efficace étant donné qu'elle devrait inclure une enquête au cas par cas pour retracer le contexte de

6

ANNEXES

la consultation. L'efficacité du contrôle ex-post de la journalisation en serait fortement réduit. Par conséquent, sans autres explications de la part des auteurs du texte, la CNPD ne peut pas souscrire à une telle solution. La CNPD estime que la formulation actuelle de ce passage est contraire à l'article 24 de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale.

101. La CNPD estime nécessaire de modifier le passage précité, en exigeant d'indiquer, pour chaque consultation, un motif d'accès. En même temps, elle salue que la disposition sous considération prévoit que la Police détermine par ailleurs « *des motifs d'accès spécifiques selon le type de mission légale* » ainsi que, dans des situations non-couvertes par ces motifs d'accès, une « *raison précise de la consultation* » doit être indiquée. Or, les auteurs du projet de loi ont omis de donner des indications, au moins dans le commentaire des articles, sur les « motifs d'accès spécifiques » envisagés. La CNPD souligne qu'une simple référence à une consultation à des fins de police judiciaire, à des fins de police administrative ou à des fins d'autres missions légales ne serait manifestement pas suffisante.
102. Le motif d'accès pourrait, par exemple, se baser sur les identifiants des enquêtes, des opérations de police et des décisions des autorités judiciaires justifiant l'accès. La CNPD rappelle que lesdits motifs d'accès

doivent permettre de retracer avec une précision suffisante la raison de l'accès aux données afin de s'assurer, dans le contexte des contrôles ponctuels et périodiques de la légitimité des accès.

103. Concernant l'accès à la partie passive du fichier central, la Commission nationale note avec intérêt que, d'une part, un accès ponctuel peut être accordé, en application de l'article 43-2, paragraphe 19, alinéa 2, ou un accès limité dans le temps pouvant être accordé nominativement à des officiers et agents de police judiciaire du service de police judiciaire ou subdivisions du service de police judiciaire, à l'alinéa 3.
104. La CNPD accueille favorablement la durée de conservation des logues de journalisation prévus à l'article 24 précité, fixée à cinq ans à l'article 43, paragraphe 5, sauf lorsqu'elles font l'objet d'une procédure de contrôle.
105. Dans l'avis relatif au fichier central, elle avait constaté que

« les mécanismes de journalisation ne permettent pas d'atteindre en pratique l'intégralité des finalités tels qu'énoncés dans la loi. Ainsi, la vérification de la licéité de chaque consultation semble difficile sur base des informations contextuelles limitées qui sont reprises dans le journal (i. e. seul une motivation générique sommaire est reprise dans le journal). »

106. La CNPD regrette que le projet de loi ne précise pas l'article 24 précité, en prévoyant le contenu des logues adaptés aux fichiers de la Police grand-ducale, en particulier relatif au motifs de consultation.
107. Elle se demande s'il ne serait pas opportun de définir les critères d'accès et les critères de journalisation de manière transversale, pour les accès aux banques de données visées à l'article 43, pour les fichiers particuliers visés à l'article 43-1 et pour le fichier central visé à l'article 43-2.
108. Ainsi, il serait nécessaire d'harmoniser les dispositions en matière de journalisation concernant les fichiers de la Police avec les modalités de contrôle des logues découlant de l'article 43, paragraphes 6 à 8.

6. Durées de conservation

109. L'article 4 de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale fixe les règles minimales en matière de délais de conservation et d'examen :

« (1) Le responsable du traitement fixe des délais appropriés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel. Les délais sont à fixer eu égard à la finalité du traitement.

(2) Le responsable du traitement établit des règles procédurales en vue d'assurer

le respect de ces délais qui déterminent les personnes intervenant au nom et pour compte du responsable du traitement dans cette procédure, y compris le délégué à la protection des données, ainsi que les délais dans lesquelles ces personnes doivent accomplir leurs tâches respectives. Les règles procédurales sont mises à la disposition de la personne concernée conformément à l'article 11 et à l'autorité de contrôle compétente sur demande de celle-ci. »

110. Dans son avis relatif au fichier central, la CNPD a déjà considéré que la disposition précitée ne reflétait pas correctement l'article 5 de la directive qu'elle est censée transposer :

« Dans son avis du 28 décembre 2017 relatif au projet de loi (n° 7168) de transposition de la directive, la CNPD avait estimé que l'article 5 de la directive n'était pas correctement transposé en droit national. Le législateur n'a cependant pas suivi l'argumentation de la CNPD. »

111. Elle avait par ailleurs relevé que « les délais de conservation ou du moins les critères applicables pour déterminer la durée de conservation ainsi que les procédures permettant la vérification régulière de la nécessité desdits délais mériteraient d'être précisés par le législateur afin de limiter au maximum la marge de manœuvre du responsable du traitement

6

ANNEXES

et garantir la transparence, l'accessibilité et la proportionnalité desdits délais ».

112. La CNPD salue le fait que l'article 43-2, paragraphes 9 à 18, contient des dispositions détaillées sur les durées de conservation applicables aux données contenues dans la partie active et la partie passive du fichier central.
- 6.1. Données contenues dans la partie active du fichier central**
113. Les données contenues dans la partie active du fichier central sont définies à l'article 43-2, paragraphe 7, ainsi que, implicitement, toute information contenue dans les procès-verbaux et rapports sauvegardés dans celui-ci conformément au paragraphe 1^{er}, y compris des catégories particulières de données à caractère personnel dans la limite de l'article 43-1, paragraphe 2. L'accès aux données est différencié suivant les finalités définies aux paragraphes 1^{er} et 2 de l'article 43-2, les règles d'accès définies notamment par les paragraphes 5, 9 et 10 de l'article 43-1 et les profils et modalités d'accès définis par la Police au sens de l'article 43-1, paragraphe 3.
114. L'article 43-2 prévoit six sous-catégories :
- 6.1.1. Les données introduites au titre de missions de police administrative et de toute autre mission dont la Police est investie par la loi**
115. En premier lieu, la CNPD s'interroge sur la définition de « *toute autre mission dont la Police est investie par la loi* » et souhaite obtenir plus d'information concernant les missions qui ne relèverait ni des missions de la police administrative, ni des missions de la police judiciaire. De plus, force est de constater que, dans la disposition sous examen et dans le commentaire des articles afférent, différentes notions sont utilisées, « *mission dont la Police est investie par la loi* », de « *missions administratives* ». Il est renvoyé aux développements précédents relatives à l'article 43 nouveau et la notion de « *fins administratives* ».
116. L'article 43-2, paragraphe 15 prévoit que « *[l]es informations et données à caractère personnel [...] dans le cadre d'une mission de police administrative ou dans le cadre d'une mission administrative dont la Police est investie par la loi, sont supprimées au plus tard après une période de dix ans après leur enregistrement dans le fichier central [...]* ». La CNPD accueille favorablement que les données soient en principe supprimées après l'écoulement dudit délai.
117. Cependant, sans connaître les « *missions administratives* », il est difficile de se prononcer sur l'adéquation de ce délai de 10 ans. La CNPD rappelle qu'il n'est pas suffisant d'invoquer « *un souci de simplification [...] ce qui évite de prévoir plusieurs exceptions de prolongation* »,

tel qu'il ressort du commentaire des articles, pour justifier un délai de conservation unifié qui de plus est de dix ans. Le commentaire des articles reste muet quant à d'éventuels aménagements prévues à ce délai maximum et en comprend que les auteurs envisagent en principe l'application standardisée de ce délai. Or, la CNPD s'interroge sur la proportionnalité du délai de 10 ans pour les missions ne relevant pas de la police administrative. Elle peut néanmoins concevoir que, tel que proposé dans la disposition sous examen, la Police fixe elle-même les durées de conservation pour les missions de police administrative et les missions découlant de lois spéciales, dans les limites du délai maximum que la disposition prévoit, en indiquant in fine « *[l]a Police peut arrêter des délais de conservation plus courts par type de rapport au sens de ce paragraphe, auquel cas elle tient un relevé dans lequel les délais spécifiques sont indiqués* ». La Commission nationale rappelle également que les dispositions légales spécifiques peuvent prévoir des délais de conservation différents qu'il convient de respecter, comme c'est le cas par exemple à l'article 25 la loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière. En tout état de cause, la restriction des accès peut réduire le risque pour les personnes concernées.

6.1.2. Les données relatives aux mineurs

118. L'article 43-2, paragraphe 15, alinéa 2, prévoit que les « informations et données à caractère personnel contenues dans le fichier central relatives à des personnes mineures en fugue sont effacées du fichier central lorsque la personne a atteint l'âge de dix-huit ans ». La CNPD peut souscrire à la solution retenue.
119. Cependant, elle s'interroge sur la proportionnalité et la nécessité d'appliquer les durées de conservation communes aux données relatives aux mineurs autres que celles relatives à des personnes mineures en fugue, notamment eu égard aux exigences de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse ainsi que de la réforme engagée dans ce domaine.

6.1.3. Les données relatives aux demandes d'entraide judiciaire internationale

120. Sur base de l'article 43-2, paragraphe 14, alinéa 1, les documents rédigées dans le cadre de ses missions de police judiciaire dans le contexte d'une demande d'entraide sont conservés pendant 20 ans dans la partie active.
121. Alors que le délai de conservation dans la partie active du fichier central ne semble pas excessif, la CNPD suggère néanmoins d'assortir ce type de documents de règles d'accès spécifiques.

6

ANNEXES

- 6.1.4. Les données relatives à la coopération policière internationale ou des « rapports aux autorités judiciaires qui n'ont pas comme objet la constatation d'une infraction pénale » qui « ne concernent pas une enquête en cours ou une infraction déterminée »**
122. L'article 43-2, paragraphe 14, alinéa 2, renvoie à l'article 43-2, paragraphe 15, alinéa 1 pour ce type de données. La CNPD renvoie aux développements plus haut concernant l'adéquation du délai maximum de conservation de 10 ans, en soulignant qu'il convient de prendre également en compte les obligations découlant d'engagements internationaux en matière de coopération policière internationale dans la détermination des durées de conservation desdites données²¹⁰.
- 6.1.5. Données relatives à la coopération policière internationale ou des « rapports aux autorités judiciaires qui n'ont pas comme objet la constatation d'une infraction pénale » qui concernent une enquête en cours ou une infraction déterminée**
123. L'article 43-2, paragraphe 14, alinéa 2, prévoit que pour ce type de données, la durée de conservation s'aligne sur celle applicable aux « *procès-verbaux ou rapports élaborés dans le cadre de l'enquête à laquelle ils se rapportent* ». La CNPD peut se rallier à cette solution.
- 6.1.6. Les données introduites au titre de missions de police judiciaire**
124. L'article 43-2, paragraphe 8, prévoit que « *[l]es données à caractère personnel et les informations prévues aux paragraphes (3) et (4) sont transmises au fichier central si l'enquête est terminée, ou si l'autorité judiciaire compétente a autorisé la transmission conformément à la loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière* ». Dans le commentaire des articles, les auteurs expliquent que ce paragraphe « *détermine le moment auquel les données peuvent être répertoriées dans le fichier central* » et justifient qu'« *[a]vec l'enregistrement d'un procès-verbal ou rapport dans le fichier central, les informations et données deviennent accessibles à l'ensemble des officiers et agents de police judiciaire de la Police qui disposent d'un droit d'accès en vertu de l'article 43-1, paragraphe 3. Or, ces informations et données peuvent être couvertes par le secret de l'enquête voire le secret de l'instruction.* ».
125. La CNPD se demande comment les données sont conservées en attendant la transmission au fichier central. Ainsi, en attendant la fin de l'enquête ou

²¹⁰ Voir par exemple, l'article 4, paragraphe 4, alinéa 1er de l'accord entre le Gouvernement du Grand-Duché de Luxembourg, le Gouvernement du Royaume de Belgique, le Gouvernement de la République fédérale d'Allemagne et le Gouvernement de la République française, concernant la mise en place et l'exploitation d'un centre commun de coopération policière et douanière dans la zone frontalière commune, signé à Luxembourg, le 24 octobre 2008.

la décision des autorités judiciaires, le procès-verbal ou le rapport est conservé par l'auteur dudit document, sans qu'il ne soit réellement possible d'en vérifier les conditions de sécurité et d'accès. En particulier, lors d'enquêtes qui durent plus longtemps, il se pose la question des modalités de conservation desdits documents, notamment s'il existe une sorte de « *fichier temporaire* » au niveau de chaque officier de police judiciaire chargé d'une enquête par le ministère public ou par un juge d'instruction.

126. Pour justifier ce décalage dans le versement du document au fichier central, les auteurs du projet de loi semblent indiquer implicitement que l'accès ne peut pas être restreint aux seuls officiers et agents de police judiciaire chargés de l'enquête. Or, dans la même disposition sous examen, conformément à l'article 43-2, paragraphe 5, alinéas 2 et 3, il est prévu que le fichier central permet de limiter l'accès aux données « *douces* » « *aux officiers de police judiciaire en charge de l'information* ». Par ailleurs, l'article 43-1, paragraphe 3, chiffre 6°, prévoit également que l'accès aux données relatives à des mineurs doivent pouvoir être limité au personnel de certains officiers ou agents de la Police. Il semblerait que le système devra permettre de restreindre l'accès nominativement à certains officiers, et il se pose alors la

question si cette solution ne pourrait pas être transposée aux données relatives à des enquêtes en cours. La gestion des accès permettrait, de l'avis de la CNPD, de respecter le secret de l'enquête et le secret de l'instruction. Si le système ne permettait pas de restreindre l'accès nominativement à certains officiers, le responsable de traitement serait confronté à des difficultés de mettre en œuvre les dispositions relatives à l'accès aux données « *douces* » et aux données relatives à des mineurs.

127. La CNPD note avec intérêt que l'article 43-1, paragraphes 9 à 13, contient des critères qui déclenchent le transfert des données de la partie active vers la partie passive du fichier central et que des règles spécifiques ont été prévues pour les données en relation avec des contraventions en application de l'article 43-1, paragraphe 17.
128. Elle salue la mention des décisions de condamnation, d'acquittement, de non-lieu ou de classement sans suite dans le fichier central, tel que prévu par l'article 43-2, paragraphe 12. Cette inscription contribue grandement à l'exactitude des données contenues dans le fichier central. Elle suggère de prévoir également qu'il soit fait mention de la réhabilitation, en particulier dans les dossiers visant plusieurs personnes physiques conservés dans la partie active.

6

ANNEXES

6.1.6.1. En l'absence de décision de justice, y compris en cas de décisions de non-lieu, de décision de classement sans suites et de décision de classement « *ad acta* »

129. La CNPD se félicite de la mise en place du retour automatisé entre la base de données des autorités judiciaires et du fichier central par le biais de l'article 43-2, paragraphe 11. En effet, il s'agit d'une recommandation contenue dans son avis relatif au fichier central. D'une part, techniquement, ce retour automatisé semble dorénavant fonctionner, et d'autre part les auteurs du projet de loi l'ont retenu pour déclencher le transfert vers la partie passive du fichier central. D'après les auteurs, « [l]e paragraphe 11 vise les décisions de non-lieu, de classements sans suites, ainsi que les affaires dans lesquelles l'auteur est resté inconnu ou les affaires prescrites qui sont mises 'ad acta' et pour lesquelles aucune décision n'est intervenue ». Enfin, la CNPD s'interroge sur le traitement identique de décisions différentes. Toutefois, elle estime que, d'une part, cette question peut être résolue au niveau du « JUCHA » et qu'il revient également au procureur d'Etat de prendre les mesures nécessaires conformément à l'article 43-2, paragraphe 13. Elle peut dès lors se satisfaire de la solution retenue à la disposition sous considération.
130. Ainsi, en l'absence d'une décision judiciaire, les données sont transmises dans la partie passive du fichier central lorsque le dossier fait l'objet d'un « *archivage* » dans l'« *traitement, dit chaîne pénale, du ministère public* », c'est-à-dire une réduction de l'accessibilité des données relatives au dossier. Dès lors, étant donné que le délai actuel de cette mesure est fixé à 3 ans, ce délai s'applique également aux données contenues dans le fichier central. La CNPD note que les réflexions sont engagées pour augmenter ce délai à 5 ans.
131. La CNPD s'interroge néanmoins sur les règles applicables en cas d'absence de retour automatisé de la part des autorités judiciaires. Elle recommande de prévoir une solution de repli lorsque le retour automatisé ne fonctionne pas.
132. À noter également que cette mesure est réversible dès lors que le dossier fait l'objet d'« *[u]ne retransmission dans la partie active du traitement, dit chaîne pénale, du ministère public donne lieu à une retransmission dans la partie active du fichier central.* » conformément à l'article 43-2, paragraphe 16, alinéa 2.

6.1.6.2. En cas de décision de condamnation coulée en force de chose jugée

133. La CNPD peut souscrire pleinement à la solution retenue à l'article 43-2, paragraphe

9, en présence d'une condamnation coulée en force de chose jugée, en ce que, d'après les termes des auteurs du projet de loi, « *la durée de conservation des informations et données dans le fichier central de la Police est liée à la durée pendant laquelle la condamnation figure au casier de la personne concernée* ». Ainsi, lors de la réhabilitation, les données sont transmises dans la partie passive du fichier central. La CNPD se demande quel traitement est réservé aux décisions visant la suspension du prononcé de la condamnation et des ordonnances pénales.

Elle comprend également que, sur base de l'article 43-2, paragraphe 9, alinéa 2, « *lorsque la réhabilitation ne concerne pas toutes les personnes condamnées, les informations et données sont maintenues en partie active jusqu'à la réhabilitation de toutes les personnes condamnées dans une affaire déterminée* » puisque les données se rapportent à des documents relatifs à une poursuite pénale. Elle peut se satisfaire du fait que « *la personne réhabilitée dans l'affaire visée ne peut plus être recherchée dans la partie active* » tout comme la solution retenue pour les victimes et témoins à l'article 43-2, paragraphe 9, alinéa 3.

6.1.6.3. En cas de décision d'acquiescement coulée en force de chose jugée

134. L'article 43-2, paragraphe 10, prévoit une transmission dans la partie passive du fichier central « *dès que la Police est informée de la décision d'acquiescement, sauf si le Procureur d'Etat ordonne leur maintien* ». Les auteurs du projet de loi se réfèrent à la législation française, en particulier à l'article 230-8 du Code de procédure pénale français. Or, à la différence dudit article 230-8, la solution par défaut retenue par les auteurs n'est pas la suppression des données, mais uniquement le transfert dans la partie passive du fichier central. De même, la législation française encadre davantage la décision du ministère public de maintenir des données relatives à des personnes acquittées dans le fichiers d'antécédents de la police judiciaire. La CNPD estime nécessaire que les droits des personnes acquittées soient mieux pris en compte, notamment d'un point de vue du droit à l'information et de limitation des finalités.

135. Elle peut suivre la solution retenue à l'article 43-2, paragraphe 10, alinéa 2, en matière de limitation de la recherche de la personne acquittée « *[s]i l'acquiescement ne concerne pas toutes les personnes impliquées dans la poursuite pénale* » et à l'alinéa 3 concernant les victimes et témoins.

6.1.6.4. Les contraventions

136. D'après l'article 43-2, paragraphe 1^{er}, alinéa 3, « *Le fichier central ne comporte pas les*

6

ANNEXES

données relatives à des personnes qui ont commis une contravention si une loi spéciale permet d'arrêter les poursuites pénales par le paiement d'un avertissement taxé et que la personne concernée s'est acquittée de l'avertissement taxé dans le délai prévu par la loi ». D'après les auteurs du projet de loi, cette disposition vise par exemple les « *avertissements taxés au sens de l'article 15 de loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques* ». En « *cas de non-paiement dans les délais légaux, un procès-verbal doit cependant être rédigé, qui se retrouvera dans le fichier central* ».

137. D'après l'article 43-2, paragraphe 17, alinéa 3, « *les informations et données à caractère personnel contenues dans le fichier central, qui ont leur origine dans des procès-verbaux ou rapports pour contraventions adressés aux autorités judiciaires, sont supprimées cinq ans après l'établissement du procès-verbal ou du rapport* ». La CNPD comprend que ce délai vaut à la fois pour la partie active du fichier central et pour la partie passive de celui-ci, notamment lorsque le dossier a été transmis à la partie passive en application de l'article 43-2, paragraphes 11 ou 13.

138. Elle peut souscrire à ces deux passages du texte sous considération pour les avertissements taxés acquittés sur base d'une loi spéciale d'une part et pour les autres contraventions d'autre part.

6.1.6.5. Les données dites « douces »

139. La CNPD peut se satisfaire des durées proposées relatives aux données de « personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles sont sur le point de commettre une infraction pénale, ainsi que les contacts ou associés qui sont suspectés d'avoir l'intention de participer à ces infractions ou d'en avoir connaissance, ainsi que les personnes qui peuvent fournir des informations sur ces infractions pénales » telles que définies à l'article 43-2, paragraphe 4, point 10°. Ainsi, conformément à l'article 43-2, paragraphe 14, alinéa 3, les données sont « transférées dans la partie passive un an après leur enregistrement dans la partie active du fichier central. Ce délai peut être prolongé d'une année supplémentaire sur décision motivée [...] ». De même, ces données « sont supprimées trois ans après leur transfert dans la partie passive » conformément à l'article 43-2, paragraphe 17, alinéa 2.

140. La CNPD s'interroge toutefois du sort des données de « personnes auxquelles il existe des motifs sérieux de croire qu'elles sont sur le point de commettre une infraction pénale » pour lesquelles l'accès a été modifié conformément à l'article 43-2, paragraphe 5, alinéa 4.

6.1.6.6. Les décisions visant les limitations du traitement ou le transfert vers la partie passive du fichier central

141. La Commission nationale salue l'insertion de l'article 43-2, paragraphe 13, qui donne la possibilité au procureur d'Etat « *d'office ou à la demande de la personne concernée* », d'ordonner le transfert de données relevant de la mission de police judiciaire dans la partie passive du fichier central ou de limiter les possibilités de rechercher la personne concernée dans la partie active. Elle relève positivement que ces décisions soient notifiées à la personne concernée et puissent faire l'objet d'un recours juridictionnel devant le Président du tribunal d'arrondissement compétent. Implicitement, cette disposition pourrait être applicable aux fichiers particuliers par la lecture combinée avec l'article 43-1, paragraphe 4 qui prévoit que « *[l]a durée de conservation [applicables aux fichiers particuliers] ne sera en aucun cas supérieure à celles qui sont applicables au fichier central* » et de l'article 43-2, paragraphe 18, qui prévoit qu'« *[a]u plus tard au moment du transfert dans la partie passive du fichier central des informations et données à caractère personnel relevant d'une mission de police judiciaire, les informations et données à caractère personnel en question qui se trouvent dans d'autres fichiers doivent être supprimées dans ceux-ci [...]* ». Or, pour des raisons liées à la sécurité juridique, la Commission nationale estime qu'il serait préférable de prévoir explicitement que le procureur d'Etat puisse ordonner les mêmes mesures concernant des données contenues dans des fichiers particuliers.

6.2. Données contenues dans la partie passive du fichier central (police judiciaire)

142. En l'état actuel, les données dans le fichier central actuel sont conservées pour une durée de 60 ans à partir de l'enregistrement de celles-ci.
143. L'article 43-2, paragraphe 17, alinéa 1^{er}, établit un délai général de 30 ans de conservation « après leur transfert dans la partie passive ».
144. L'article 43-2, paragraphe 17, alinéa 4, prévoit la possibilité, pour les autorités judiciaires, de prolonger la durée de conservation « *en raison d'une demande de révision en cours* ».
145. De manière générale, la CNPD s'interroge toujours sur la proportionnalité de ce délai de 30 ans, qui s'ajoute à la durée de conservation dans la partie active du fichier central.
146. Premièrement, elle suggère de prévoir un mécanisme de revue périodique de la nécessité et de la proportionnalité de la conservation des données sous la direction des autorités judiciaires conformément à l'article 4 de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale qui prévoit, d'une part que le responsable de traitement « *fixe des délais appropriés pour l'effacement des données à caractère personnel ou pour*

6

ANNEXES

la vérification régulière de la nécessité de conserver les données à caractère personnel » et d'autre part « établit des règles procédurales en vue d'assurer le respect de ces délais ».

147. Deuxièmement, elle propose que le législateur fixe des délais de conservation moins longs pour la partie passive du fichier central, avant tout pour les données relatives à des affaires pénales ayant abouties à des décisions d'acquiescement et de non-lieu. Dans ce cas, il pourrait être laissé à l'appréciation des autorités judiciaires, pour des raisons liées à l'affaire en question, d'ordonner des délais de conservation plus longues, à l'instar du retour écrit de la part des autorités judiciaires en matière de « demande de révision en cours ». La CNPD fait observer qu'avec la mise en place généralisée « e-justice », le besoin d'avoir accès aux documents de la police en matière de révision deviendra moins évident, et il pourra, à ce moment, être envisagé de supprimer les données au niveau de la police dans des délais pour courts.
148. Dans la même logique, il serait également envisageable de définir des délais différents pour d'autres d'infractions pénales, notamment en lien avec la gravité des faits et de la sanction pénale envisageable.
149. Par ailleurs, pour les données relatives à l'entraide, la combinaison de la durée de conservation dans la partie active de 20 ans, avec la durée de conservation proposée pour la partie passive de 30 ans, résulte dans une durée de conservation totale de 50 ans avant un éventuel archivage définitif au sens de la loi du 17 août 2018 sur l'archivage. Il conviendrait éventuellement d'adapter la durée de conservation dans la partie passive, alors que la durée totale semble disproportionnée.
150. Ainsi, la CNPD suggère que, en suivant la logique de la procédure mise en place à l'article 43-2, paragraphe 13, de prévoir également la possibilité, pour les autorités judiciaires compétentes, d'ordonner l'effacement de données de la partie passive du fichier central.

6.3. Les données introduites dans un fichier particulier

151. Concernant les fichiers particuliers ne disposant pas de dispositions légales définissant les durées de conservation, il convient de différencier les cas de figure suivants :
- Données contenues dans la partie active du fichier particulier accessibles suivants les règles d'accès définies à l'article 43-1, paragraphe 3 en application de durées de conservation fixées par le responsable de traitement conformément à l'article 43-1, paragraphe 4 ;

152. La Commission nationale note avec intérêt qu'en application de l'article 43-1, paragraphe 4, les durées de conservation dans la partie active des fichiers particuliers ne devraient pas dépasser les durées de conservation applicables à la partie active du fichier central, sauf en cas de disposition légale contraire prévoyant des durées de conservation plus longues. Elle constate que ladite disposition ne contient pas de critères pour la détermination de la durée de conservation et laisse ainsi une marge d'appréciation très large à la Police grand-ducale en se référant uniquement à une durée de conservation maximale. De plus, elle regrette que l'article 43-1, paragraphe 4, ainsi que le commentaire des articles restent muets sur les « règles procédurales » que la Police grand-ducale entend se donner pour se conformer à l'article 4, paragraphe 2, de la loi du 1^{er} août 2018 précitée et à l'article 5 de la directive en ce qui concerne les fichiers particuliers.
- Données contenues dans la partie passive du fichier particulier, à défaut de pouvoir être transférées dans la partie passive du fichier central, conformément à l'article 43-2, paragraphe 18, alinéa 2;
 - Données relatives à des « traces prélevées dans le cadre d'enquêtes où les auteurs des faits sont restés inconnus » contenues dans la partie passive du fichier particulier, conformément à l'article 43-2, paragraphe 18, alinéa 3;
153. La Commission nationale peut souscrire à la solution retenue dans les deux cas de figure. Elle suggère néanmoins de prévoir explicitement leur transfert dans la partie passive du fichier particulier en question et de limiter les finalités à ces celles visées à l'article 43-2, paragraphe 19, applicable à la partie passive du fichier central.
- Données contenues dans la partie active du fichier particulier ne disposant pas de partie passive ayant atteint, en principe, les durées de conservation, conformément à l'article 43-2, paragraphe 18, alinéa 2.
154. L'article 43-2, paragraphe 18, alinéa 2 semble ouvrir la voie à des fichiers particuliers qui ne disposeraient pas de « possibilité d'archivage », c'est-à-dire, dans la compréhension de la CNPD d'une partie passive. Cependant, la CNPD s'interroge sur la définition des accès à des données contenues dans un fichier particulier visé par ledit alinéa ne disposant pas de partie passive.
155. D'un point de vue formel, l'article 43-2, paragraphe 18, alinéa 2, fait état de la « possibilité d'archivage » et de « durées d'archivage ». Or, la CNPD relève que cette terminologie peut créer une confusion avec la loi du 17 août 2018 relative à l'archivage, alors que la partie passive d'un fichier central ne constitue pas une mesure d'archivage définitif au sens de ladite loi. Par conséquent, il serait préférable de se référer à la transmission

6

ANNEXES

de données dans la partie passive du fichier particulier concerné et aux « *durées de conservation* ».

156. Concernant les fichiers particuliers mises en œuvre sur le fondement d'un instrument juridique distinct, il convient de se référer aux dispositions relatives aux durées de conservation y définies. La Commission nationale suggère que, suite à l'adoption du présent projet de loi, le législateur aligne au besoin ces dispositions légales aux principes dégagés dans les dispositions sous considération.

157. La loi du 17 août 2018 relative à l'archivage peut exiger de conserver des documents contenus dans le fichier central ou les fichiers particuliers au-delà des durées de conservation discutées dans le présent projet de loi, à savoir les documents susceptibles de faire l'objet d'un archivage définitif et, le cas échéant, d'un versement aux archives nationales. Or, la CNPD rappelle que l'accès doit être en principe impossible, à l'exception stricte pour la mise en œuvre des opérations de traitement de données pour les finalités visées à ladite loi du 17 août 2018, principalement le conditionnement en préparation à l'archivage définitif.

7. La modification de l'article 509-1 du Code pénal

158. Le projet de loi prévoit de modifier l'article 509-1 du Code pénal, en y insérant, aux

termes des auteurs du projet de loi, une disposition pénale « *en matière de violations des droits d'accès, et ce à l'égard de toutes les autorités étatiques et entités privées* », en tenant compte, de ce que la CNPD en comprend, de l'évolution jurisprudentielle à cet égard. Elle rappelle néanmoins que ceci n'enlève en rien à la responsabilité du responsable de traitement de notamment mettre en place des systèmes de contrôle des accès ex ante, des revues des logues et la formation de ses agents.

8. Les dispositions transitoires

159. La CNPD rappelle que l'article 63, paragraphe 1, de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale prévoit des dispositions transitoires et de mise en conformité :

« (1) À titre exceptionnel et lorsque cela exige des efforts disproportionnés, les systèmes de traitements de données à caractère personnel automatisés installés avant le 6 mai 2016 sont mis en conformité avec l'article 24 au plus tard le 6 mai 2023.

(2) Par dérogation au paragraphe 1^{er}, et dans des circonstances exceptionnelles, un système donné de traitement de données à caractère personnel automatisé visé au paragraphe 1^{er} peut être mis en conformité avec l'article 24 jusqu'à une date butoir à déterminer par une décision du Gouvernement en conseil et située

après le 6 mai 2023 lorsque, à défaut de cela, de graves difficultés se posent pour le fonctionnement du système de traitement automatisé en question. La date butoir ne peut être fixée au-delà du 6 mai 2026.»

160. L'article 7, alinéas 1 et 2, du projet de loi sous considération prévoit quant à lui que

« Les fichiers autres que le fichier central de la Police établis avant l'entrée en vigueur de la présente loi sont mis en conformité avec l'article 43-1 de la présente loi au plus tard le 6 mai 2023.

Par dérogation à l'alinéa 1er, lorsque cela exige des efforts disproportionnés et l'intervention de ressources externes, les fichiers autres que le fichier central peuvent être mis en conformité avec l'article 43-1 de la présente loi jusqu'au 6 mai 2026.»

161. La CNPD s'interroge sur la compatibilité entre les deux dispositions transitoires alors que le présent projet de loi ne devrait en principe uniquement préciser et clarifier la mise en œuvre des obligations découlant de la loi précitée du 1^{er} août 2018. La disposition transitoire de la loi précitée du 1^{er} août 2018 se limite en effet à permettre un délai de mise en conformité avec les obligations découlant de l'article 24 de ladite loi relatif à la journalisation pour des fichiers créés avant le 6 mai 2016.

162. La CNPD s'interroge aussi sur l'absence d'exigences procédurales prévues à l'article 7, alinéa 2, du projet de loi à la lumière des contraintes posées par la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale.

163. Dans le commentaire des articles, les auteurs du projet de loi expliquent, en prenant appui sur les délais prévus à l'article 63 précité, que,

« Comme des efforts de programmation devront donc être réalisés au plus tard pour ces dates, il s'avère opportun de prévoir les mêmes délais pour les autres adaptations à prévoir dans le cadre du présent projet de loi, qui exige des travaux considérables sur le plan technique, le recrutement de personnel hautement spécialisé et l'intervention de ressources externes.

Il convient également de préciser que la Police dispose de certaines banques de données spécialisées qui ont été acquises auprès de fournisseurs internationaux, tels les logiciels de comparaison des empreintes digitales ou d'empreintes génétiques, ou d'autres applications utilisées notamment par le Service de police judiciaire en matière de gestion et d'exploitation des traces trouvées sur les lieux du crime. Les fournisseurs doivent de toute façon adapter leurs logiciels au plus tard pour l'année 2026, il convient donc de fixer la même date pour la mise

6

ANNEXES

en conformité par rapport aux dispositions de la présente loi, afin d'éviter des coûts disproportionnés ou le risque de ne pas pouvoir effectuer les interventions nécessaires dans le délai fixé. »

164. La CNPD avait estimé, dans son avis relatif au fichier central, que :
- « Au regard des éléments dont dispose la CNPD actuellement quant à la structure et la configuration du fichier central, elle tient à rappeler que la Police grand-ducale ne pourra pas se référer derrière des contraintes techniques pour justifier une non-conformité. Il incombe à ce moment au responsable du traitement de prendre toutes les mesures nécessaires pour assurer qu'il soit en mesure de respecter pleinement les droits des personnes concernées - même si ceci nécessite le développement d'un système informatique. »*
165. Le même constat est valable pour les éventuels fichiers existants exploités par la Police grand-ducale. À cet égard, elle se demande en quoi les considérations techniques invoquées, notamment *« l'intervention de ressources externes »* constituent des *« circonstances exceptionnelles »* et qu'une adaptation jusqu'au 6 mai 2023 poserait de *« graves difficultés [...] pour le fonctionnement du système de traitement automatisé en question »*.
166. La CNPD considère qu'il serait préférable d'aligner les dispositions transitoires dans le projet de loi, en particulier en les limitant aux fichiers créés avant le 6 mai 2016 et en restreignant la portée de celle-ci à l'article 43-1, paragraphe 5 relatif à la journalisation à *« titre exceptionnel et lorsque cela exige des efforts disproportionnés »*.
167. La Commission nationale rappelle que les considérations techniques ne doivent pas justifier à elles seules de longues périodes de transition. À l'instar des homologues étrangers, l'encadrement légal ou réglementaire des traitements des données ne doit pas être considéré comme un frein à l'efficacité de l'action de la Police grand-ducale, mais peut accompagner et guider le travail des autorités répressives au quotidien en fournissant des règles claires et transparentes à tous les acteurs impliqués et personnes concernées.
168. En particulier pour les fichiers complexes, de par les volumes des données traitées, des formats utilisés et des interconnexions de ces fichiers, la CNPD estime qu'il est possible de déterminer d'ores et déjà qui les utilise et à quelles finalités, quelles données sont stockées et pour combien de temps, comment le contrôle d'accès a priori et a posteriori est effectué. Ainsi, la CNPD estime qu'il est possible d'encadrer, par un texte législatif ou réglementaire, ces fichiers sans aucunement entraver l'efficacité des autorités répressives.
169. Les auteurs du projet de loi estiment que la Police grand-ducale a besoin d'une

flexibilité accrue dans la création de fichiers, sans recourir à une base légale. Comme exposé, la CNPD peut suivre ce raisonnement pour une série de fichiers en tant que prolongation du fichier central ou de fichiers particuliers disposant d'une base légale séparée. Cependant, pour ces fichiers, plus versatiles et plus facilement adaptables, il est difficile d'admettre une non-conformité pendant une durée allant de 3 à 6 ans, y compris une non-conformité limitée aux obligations de journalisation.

170. La CNPD comprend que le « *nouveau* » fichier central sera opérationnel à l'entrée en vigueur de la loi découlant du présent projet de loi, c'est-à-dire six mois après la publication de ladite loi au Journal officiel du Grand-Duché de Luxembourg. L'article 7, alinéa 3, du projet de loi prévoit que l'accès au fichier central existant serait limité au officiers et agents de police judiciaire pendant un an après l'entrée en vigueur de la loi. L'article 7, alinéas 4 à 7, du projet de loi régit la migration et l'interaction entre le fichier central existant à ce jour et le « *nouveau* » fichier central. Ces dispositions n'appellent quant à elles pas d'observations particulières de la part de la CNPD.

171. En tout état de cause, la CNPD rappelle que les efforts de mise en conformité pour les systèmes en place doivent avancer, en particulier en mettant en œuvre les recommandations issues de l'avis de la CNPD et de l'avis de l'IGP de 2019.

172. En conclusion, la CNPD salue le projet de loi qui encadre de manière détaillée le fichier central. Même si elle peut convenir qu'il n'est pas nécessaire d'encadrer individuellement chaque traitement de données mis en œuvre par la Police dans l'exercice de ses missions de police judiciaire ou de police administrative, elle réitère sa conviction que, dans le fonctionnement d'une société démocratique, il serait préférable d'encadrer par des dispositions légales ou réglementaires les traitements de données les plus intrusifs, de par le nombre de personnes concernées et de par la sensibilité des données traitées.

173. Ainsi décidé à Belvaux en date du 16 mars 2021.

174. La Commission nationale pour la protection des données

175. Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

**Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7795 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19.
(Délibération n°14/AV11/2021 du 29/03/2021)**

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 25 mars 2021, Madame la Ministre de la Santé a saisi la Commission nationale d'une demande d'avis sur le projet de loi n°7795 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 (ci-après le « projet de loi n°7795 »).

Il ressort de l'exposé des motifs que le présent projet de loi vise notamment à permettre au secteur Horeca à partir du 7 avril 2021 d'ouvrir ses terrasses sous des conditions très strictes comme, entre autres, une « *nouvelle formalité obligatoire importante pour le contact tracing en cas de contagion épidémiologique, à savoir l'obligation pour les établissements concernés de tenir un registre de leurs clients.* »

La CNPD constate en effet que l'article 2 du projet de loi n°7795 prévoit de modifier la teneur actuelle de l'article 2 de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 (ci-après : « la loi modifiée du 17 juillet 2020 »), de sorte que son paragraphe (4) prévoit dorénavant ce qui suit :

« *Les établissements visés au paragraphe 1^{er}, ainsi que les restaurants et bars des établissements d'hébergement doivent obligatoirement tenir un registre de leurs clients qui contient les données suivantes :*

- 1° le(s) prénom(s) et nom du client déclarant ;*
- 2° l'adresse de résidence du client déclarant ;*
- 3° un numéro de téléphone du client déclarant, et le cas échéant, une adresse e-mail.*

Ces données doivent être collectées et enregistrées par les établissements à l'arrivée des clients et conservées pendant une durée de trois semaines à partir de la collecte, afin de faciliter toute recherche de contact ultérieure en cas de contagion épidémiologique. L'accès des établissements visés au paragraphe 1^{er} et des restaurants et bars des établissements

d'hébergement est conditionné à la communication par le client des données visées à l'alinéa 1^{er}.

Ces données sont communiquées, conformément à l'article 5, paragraphe 2, dernier alinéa, au directeur de la Santé ou à son délégué en cas d'exposition à haut risque. Elles doivent être supprimées après trois semaines par les établissements et ne peuvent en aucun cas être utilisées à d'autres fins que celles prévues à l'alinéa précédent.»

En vertu du nouvel alinéa ajouté par les auteurs du projet de loi n°7795 à l'article 5 paragraphe (2) de la loi modifiée du 17 juillet 2020, les responsables des établissements de restauration et de débit de boissons et des établissements d'hébergement qui disposent d'un restaurant ou d'un bar (ci-après : « les établissements ») doivent transmettre « *sur demande, au directeur de la Santé ou à son délégué les données prévues à l'article 2, paragraphe 4, des personnes qui ont subi une exposition à haut risque en raison d'une des situations visées à l'article 1^{er}, point 5°.* »

Le commentaire des articles ne donne pas de précisions supplémentaires sur les nouvelles dispositions précitées.

La Commission nationale tient à souligner à titre préliminaire que la collecte et l'enregistrement des données précitées dans le registre que doivent tenir les établissements (ci-après : le registre»), qu'il s'agisse d'un registre sous forme papier ou sous forme électronique, constitue un

traitement de données à caractère personnel soumis aux règles prévues par le RGPD.

1. Quant au principe de la limitation des finalités

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. Il ressort des nouveaux articles 2 paragraphe (4) et 5 paragraphe (2) dernier alinéa de la loi modifiée du 17 juillet 2020 que la collecte par les établissements des données à caractère personnel des clients et l'enregistrement subséquente dans leur registre servent à faciliter toute recherche de contact ultérieure par la Direction de la Santé des personnes qui ont subi une exposition à haut risque en raison d'une des situations visées à l'article 1^{er}, point 5° de ladite loi, comme par exemple avoir eu un contact, sans port de masque, face-à-face pendant plus de quinze minutes et à moins de deux mètres avec une personne infectée.

La CNPD ne dispose pas des compétences scientifiques et épidémiologiques nécessaires afin d'évaluer la plus-value que présente la tenue d'un tel registre en termes de contact tracing mis en oeuvre par la Direction de la Santé. Néanmoins, dans la mesure où les conditions d'ouverture des terrasses sont restrictives¹ et en tenant compte de ce que les personnes infectées sont de toute façon obligées en vertu de l'article 5 paragraphe (1) de la loi modifiée du 17 juillet 2020 de renseigner la Direction de la santé sur l'identité des personnes avec lesquelles elles ont eu dans les

6

ANNEXES

dernières quarante-huit heures des contacts susceptibles de générer un haut risque d'infection, elle se demande dans quel cas précis la Direction de la Santé demanderait à un établissement de lui transmettre des données à caractère personnel figurant dans son registre.

La Commission nationale félicite les auteurs du projet de loi n°7795 sous examen d'avoir prévu dans le corps du texte² que les données collectées par les établissements ne peuvent en aucun cas être utilisées à d'autres fins que la communication, conformément à l'article 5, paragraphe 2, dernier alinéa de la loi modifiée du 17 juillet 2020, à la Direction de la Santé en cas d'exposition à haut risque. Toute autre utilisation, comme par exemple à des fins de marketing ou de prospection, sera donc strictement interdite et les données collectées dans le contexte de la pandémie ne pourront en aucun cas être ajoutées dans la base de données des clients, les cas échéant, déjà existante dans l'établissement, ni être fournies à d'autres entreprises.

2. Quant au principe de minimisation des données

En fonction du principe de minimisation des données (article 5 paragraphe (1) lettre c) du RGPD), les données personnelles collectées doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

A cet égard, la CNPD se demande d'un côté si toutes les données personnelles que les

établissements sont obligés de collecter, c'est-à-dire le prénom, nom, l'adresse de résidence, un numéro de téléphone, et le cas échéant, une adresse e-mail du client déclarant, sont vraiment nécessaire à la finalité poursuivie du traçage des contacts. Est-ce que la collecte du nom et prénom, ainsi qu'un seul moyen de contact (téléphone ou adresse e-mail) ne serait pas suffisante dans ce contexte ?

D'un autre côté, si le but de la tenue du registre et d'une éventuelle transmission des données à caractère personnel y figurant par les établissements à la Direction de la Santé, est d'identifier les clients, voire le personnel, qui étaient en contact direct avec une personne infectée, faute de précision dans le commentaire des articles, la CNPD se pose la question si l'indication du jour, de l'heure d'arrivée du client et éventuellement le numéro de table serait nécessaire au regard de la finalité du contact tracing. En plus, la date indiquée à laquelle les données ont été collectées est primordiale en vue de pouvoir déterminer la date de suppression des données après trois semaines par l'établissement, conformément au nouvel article 2 paragraphe (4) alinéa 2 de la loi modifiée du 17 juillet 2020.

La CNPD se demande par ailleurs si l'obligation de communication des données visées à l'alinéa 1er du nouveau paragraphe (2) de l'article 2 de la loi modifiée du 17 juillet 2020 s'impose à chaque personne assise sur une même table ou uniquement à une personne par table.

Finalement, la Commission nationale tient à insister que lors de la collecte des données, les

établissements ne peuvent pas procéder à un contrôle d'identité de la personne, par exemple en demandant de produire un document d'identité. Par contre, elle estime qu'une sorte de « Plausibilitätsprüfung »³ serait approprié, dans le but de contrôler uniquement si les données indiquées sont complètes, plausibles et non pas imaginaires à première vue (par exemple si un client indiquerait comme adresse email mickeymouse@...).

3. Quant au principe de la limitation de la conservation des données

En ce qui concerne la durée de conservation des données à caractère personnel conformément à l'article 5 paragraphe (1) lettre e) du RGPD, ladite durée ne doit pas excéder celle qui nécessaire au regard des finalités pour lesquelles les données sont traitées.

L'alinéa 2 du nouvel article 2 paragraphe (4) de la loi modifiée du 17 juillet 2020 prévoit dans ce contexte que les données collectées et enregistrées par les établissements à l'arrivée des clients doivent être conservées pendant une durée de trois semaines à partir de leur collecte.

La CNPD note toutefois que les personnes infectées sont uniquement obligées en vertu de l'article 5 paragraphe (1) de la loi modifiée du 17 juillet 2020 de renseigner la Direction de la santé sur l'identité des personnes avec lesquelles elles ont eu des contacts susceptibles de générer un haut risque d'infection « *dans la période qui ne peut être supérieure à quarante-*

huit heures respectivement avant l'apparition des symptômes ou avant le résultat positif d'un test diagnostique de l'infection au virus SARS-CoV-2. »

Comme susmentionné, si la finalité de la tenue du registre et d'une éventuelle transmission des données à caractère personnel y figurant à la Direction de la Santé, est d'identifier les individus qui étaient en contact avec une personne infectée, la CNPD se demande pourquoi les établissements sont tenus de conserver leurs registres pendant trois semaines, alors que le traçage des contacts mis en oeuvre par la Direction de la Santé se limite aux deux jours précédant l'apparition des symptômes ou le résultat positif d'un test diagnostique de l'infection au virus SARS-CoV-2. En l'absence de précisions dans le commentaire des articles, la CNPD ne peut pas apprécier si la durée de conservation de trois semaines est proportionnée par rapport à la finalité poursuivie.

Par ailleurs, la CNPD constate que la durée de conservation figure à la fois à l'alinéa 2, ainsi qu'à l'alinéa 3 du nouvel article 2 paragraphe (4) alinéa 2 de la loi modifiée du 17 juillet 2020. Ainsi, elle suggère de la biffer à un des deux endroits.

4. Quant au droit à l'information des personnes concernées

Conformément à l'article 13 du RGPD, toute une série d'informations est à fournir à la personne concernée au moment de la collecte des données à caractère personnel auprès d'elle.

6

ANNEXES

Cette information doit ainsi être délivrée aux clients au moment où les établissements collectent leurs données, et ceci sous un format facilement accessible (comme par exemple une mention d'information intégrée sur le formulaire papier / électronique à compléter par le client ou un panneau d'affichage visible à l'entrée de l'établissement).

Cette mention d'information doit par ailleurs être rédigée en des termes précises et simples.⁴ Sous réserve de ses commentaires susmentionnés, la CNPD est d'avis que cette mention devrait au moins comprendre les éléments suivants :

- l'identité et les coordonnées de l'établissement ;
- l'objectif de la collecte des données (faciliter toute recherche de contact ultérieure en cas de contagion épidémiologique par la Direction de la Santé) ;
- la base juridique du traitement (la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19) ;
- la durée de conservation des données (trois semaines) ;
- les droits dont disposent les clients (notamment le droit d'accès et de rectification, ainsi que le droit d'introduire une réclamation auprès de la CNPD) ; les éventuelles destinataires (sur demande à la Direction de la santé concernant les personnes qui ont subi une exposition à haut risque).
- les éventuelles destinataires (sur demande à la Direction de la santé concernant les

personnes qui ont subi une exposition à haut risque).

5. Quant aux mesures de sécurité

Conformément à l'article 32 paragraphe (1) du RGPD, le responsable du traitement doit mettre en oeuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pour les droits et libertés des personnes concernées.

Plus concrètement, ces mesures doivent garantir que les données ne seront accessibles qu'aux personnes autorisées (confidentialité), qu'elles seront disponibles en cas de demande par la Direction de la santé (disponibilité) et qu'elles n'auront pas été modifiées après leur collecte (intégrité).

En cas de tenue d'un registre sous format papier, il serait recommandé de mettre à disposition des formulaires individuels que les clients peuvent remplir et remettre directement à l'établissement. Par contre, si l'établissement souhaite travailler avec un seul formulaire reprenant l'ensemble des données de ses différents clients, il doit en principe le remplir lui-même (sur les indications verbales des clients). Les formulaires remplis (constituant le registre) devraient être conservés dans un lieu sécurisé (par exemple une armoire ou pièce fermée à clef) et afin de garantir la confidentialité des données collectées, l'établissement devra éviter que des clients puissent, le cas échéant, avoir accès aux coordonnées d'autres clients présents au même moment.

En cas de tenue d'un registre sous format électronique, la CNPD recommande de sécuriser l'accès au système d'information notamment avec un mot de passe « robuste » et de ne pas stocker les données collectées sur des matériels non sécurisés (comme par exemple des clés USB sans mots de passe).

Ainsi décidé à Belvaux en date du 29 mars 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

Troisième avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale. (Délibération n°16/AV12/2021 du 28 avril 2021)

Conformément à l'article 46, paragraphe 1^{er}, 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 la « loi du 1^{er} 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 ».

Le 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 »)²¹¹.

En date du 17 avril 2020, la Commission nationale a rendu son avis complémentaire sur l'amendement gouvernemental au projet de loi²¹², approuvé par le Conseil de gouvernement dans sa séance du 20 mars 2020.

En date du 3 mars 2021, la Commission nationale a rendu son deuxième avis complémentaire suite aux amendements relatifs au projet de loi²¹³, adoptés par la Commission de la Sécurité intérieure et de la Défense adoptés le 19 novembre 2020.

Le 29 mars 2021, la Commission de la Sécurité intérieure et de la Défense a adopté une série d'amendements relative au projet de loi (ci-après les « amendements »).

Dans la mesure où les amendements concernent des dispositions qui ont été commentées par la CNPD dans ses avis précités des 28 février, 17 avril 2020 et 3 mars 2021 celle-ci s'autosaisit pour les aviser.

- Ad Amendement 1

L'Amendement 1 a pour objet de modifier le paragraphe (3) de l'article 43bis nouveau de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

Il y a lieu de regretter que les remarques de la CNPD n'aient pas été prises en considération par les auteurs du projet de loi en ce qui

²¹¹ Avis de la Commission nationale pour la protection des données 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.

²¹² Avis complémentaire de la Commission nationale pour la protection des données 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.

²¹³ Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, délibération n°8/AV7/2021 du 3 mars 2021.

concerne ses observations soulevées dans son avis du 3 mars 2021, à savoir que « le projet de loi sous examen prévoit actuellement que seul 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. Dans l'hypothèse où ledit système serait étendu à d'autres territoires communaux, ne faudrait-il pas prévoir un système qui ne reposerait pas que sur la seule initiative du directeur général de la Police grand-ducale ? »²¹⁴.

La Commission nationale réitère de telles considérations.

- Ad Amendement 3

Cet amendement a pour objet de modifier le paragraphe (11) de l'article 43bis nouveau de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

Cet amendement introduit de nouvelles dispositions qui fixent la durée de conservation des images issues du système de vidéosurveillance et traitées à des fins d'« analyse du déroulement de l'intervention et de la formation interne » à une période « maximale de dix ans ».

Cet amendement a encore pour objet d'introduire un deuxième alinéa au paragraphe (11) de l'article précité. Les dispositions ajoutées disposent que « [s]i les images utilisées pour

l'analyse du déroulement de l'intervention et la formation interne permettent d'identifier directement une personne concernée, des techniques de masquage irréversibles doivent être utilisées à des fins d'anonymisation ».

Ces nouvelles dispositions soulèvent les observations suivantes de la CNPD.

- Sur la notion de données à caractère personnel

En ce qui concerne les dispositions relatives aux techniques de masquage irréversibles, les auteurs du projet de loi précisent, à ce sujet, que « dans le contexte spécifique de séquences d'images, il convient d'entendre par « directement identifiable » toute personne qui peut être identifiée directement et sans équivoque par référence à un ou plusieurs éléments spécifiques propres à son identité physique, alors que les autres identifiants prévus par la définition de « données à caractère personnel » dans la loi du 1^{er} 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 ne s'appliquent pas aux images ».

Or, il convient de rappeler que l'article 2, paragraphe (1), point 1^o, de la loi du 1^{er} 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, définit la notion de « données à caractère personnel » comme « toute information se rapportant à une

²¹⁴ Délibération n°8/AV7/2021 du 3 mars 2021, point 2 « Sur l'avis du Syndicat des villes et communes luxembourgeoises », page 5.

6

ANNEXES

personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (souligné dans le texte par la CNPD).

Dans le contexte de la vidéosurveillance, il y a lieu de relever qu'un tel système est susceptible d'entraîner la collecte d'informations picturales de personnes entrant dans l'espace surveillé qui sont identifiables sur la base de leur apparence ou d'autres éléments spécifiques²¹⁵. De telles informations sont à qualifier de données à caractère personnel car elles permettent d'identifier directement ou indirectement des personnes entrant dans l'espace surveillé.

Dès lors, une image issue d'un système de vidéosurveillance qui contiendrait des éléments permettant d'identifier directement ou indirectement une personne physique est à considérer comme une donnée à caractère personnel.

Le fait que les personnes concernées puissent être identifiées directement ou indirectement n'a pas d'incidence quant au fait que les informations qui permettent de les identifier soient à qualifier de données à caractère

personnel. De même que les éléments indiqués dans la définition visée audit article 2, paragraphe (1), point 1°, et énumérés après « notamment » le sont à titre d'exemples non-exhaustifs, l'adverbe « notamment » étant, ici, de nature indicative.

Sur base de leurs commentaires, les auteurs du projet de loi semblent donc procéder à une interprétation erronée de la notion de données à caractère personnel. Le texte sous avis devrait alors être modifié, de sorte à refléter la définition telle que prévue à l'article 2, paragraphe (1), point 1°, de la loi du 1^{er} 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.

- Sur les notions de pseudonymisation et d'anonymisation

Les auteurs du projet de loi entendent prévoir que des techniques de masquage irréversibles seront utilisées à des fins d'anonymisation. Cependant, d'après le commentaire des auteurs du projet de loi, la Commission nationale comprend que ces techniques ne permettraient pas une anonymisation des données à caractère personnel car lesdites techniques ne viseraient que l'« anonymisation » des informations qui permettraient d'identifier directement une personne concernée.

Or, il y a lieu d'attirer l'attention des auteurs du projet de loi sur le fait que l'anonymisation ne doit pas être confondue avec la pseudonymisation.

²¹⁵ Voir lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo, adoptée le 29 janvier 2020 par le Comité Européen de la Protection des Données, point 2.1. « Données à caractère personnel », page 6.

En ce qui concerne l'anonymisation, bien que cette notion ne soit pas définie par la loi du 1^{er} 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 relever que le considérant 21 de la directive (UE) 2016/680 du parlement européen et du conseil, 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, énonce qu'« [i]l n'y a (...) pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. ».

L'anonymisation est donc 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 de manière irréversible.

En ce qui concerne la pseudonymisation, l'article 2, paragraphe (2), point 5^o, de la loi du 1^{er} août 2018 précitée dispose qu'elle consiste en un « *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 ». La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. Les données concernées conservent donc un caractère personnel.

Dès lors, si l'intention était d'anonymiser les données à caractère personnel issues d'un système de vidéosurveillance, alors les techniques de masquage irréversibles devront s'appliquer à toutes les informations qui permettent d'identifier directement ou indirectement une personne concernée. *A contrario*, si seules les informations permettant d'identifier directement une personne concernée sont soumises aux dites techniques, alors ce procédé sera à qualifier de pseudonymisation. En effet, dans un tel cas, il sera encore possible d'identifier indirectement les personnes concernées.

En outre, il y a lieu d'attirer l'attention des auteurs du projet de loi sur le fait que si les données devaient être anonymisées alors les règles de la protection des données n'auront pas vocation à s'appliquer. Cela signifie que le principe de limitation de la conservation ne devra pas être

6

ANNEXES

respecté et qu'une durée de conservation ne devra donc pas figurer dans le projet de loi sous avis.

La CNPD estime, dès lors, nécessaire que les auteurs du projet de loi clarifient ces dispositions et utilisent les notions appropriées d'un point de vue de la protection des données. A ce titre, la Commission nationale suggère aux auteurs du projet de loi de s'inspirer des dispositions belges, en ce qu'elles prévoient qu'après anonymisation, « *les informations et données à caractère personnel collectées au moyen de caméras* »²¹⁶ « *peuvent être utilisées à des fins didactiques et pédagogiques dans le cadre de la formation des membres des services de police* »²¹⁷.

Ainsi décidé à Belvaux en date du 28 avril 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

²¹⁶ Article 25/6 de la loi modifiée sur la fonction de police du 5 août 1992.

²¹⁷ Article 25/7, paragraphe (2), de la loi modifiée sur la fonction de police du 5 août 1992.

Conformément à l'article 46, paragraphe 1^{er}, 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 1^{er} 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 1^{er} 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 ».

Par courrier en date du 23 avril 2021, le Ministre de la Sécurité intérieure a saisi la Commission nationale d'une demande d'avis relative à l'avant-projet de règlement grand-ducal relatif à la composition et au fonctionnement de la commission consultative pour l'évaluation de la vidéosurveillance, telle que prévue à l'article

Avis de la Commission nationale pour la protection des données relatif à l'avant-projet de règlement grand-ducal relatif à la composition et au fonctionnement de la commission consultative pour l'évaluation de la vidéosurveillance.

(Délibération n°17/AV13/2021 du 7/05/2021)

43bis paragraphe (3) du projet de loi n°7498 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale (VISUPOL) (ci-après l'« avant-projet de règlement grand-ducal »).

Les auteurs de l'avant-projet de règlement grand-ducal proposent de prévoir que ladite commission consultative soit notamment composée d'un représentant de la Commission nationale. La CNPD comprend que sa participation envisagée au sein de ladite commission consultative serait justifiée sur base de son expertise en la matière, ce qu'elle salue. Or, elle s'interroge sur les questions ayant trait à son indépendance et les risques de conflits d'intérêt qui pourraient surgir.

En effet, suivant l'article 27, paragraphe (1), de la loi du 1^{er} 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 peut être consultée « a) lorsqu'une analyse d'impact relative à la protection des données, telle qu'elle est prévue à l'article 26, indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour

6

ANNEXES

atténuer le risque, ou b) lorsque le type de traitement, en particulier, en raison de l'utilisation de nouveaux mécanismes, technologies ou procédures, présente des risques élevés pour les libertés et les droits des personnes concernées ».

Ainsi, qu'advierait-il, si la Commission nationale se verrait saisie par la Police grand-ducale d'une consultation préalable dans les cas visés à l'article 27 de la prédite loi et qu'elle considérerait que le traitement constituerait, le cas échéant, une violation de la loi du 1^{er} août 2018 précitée ?

Dans de tels cas, se posent les questions de l'indépendance de la CNPD et d'éventuels conflits d'intérêts qui pourraient naître a posteriori si la CNPD devait se prononcer, en tant que membre de la commission consultative pour l'évaluation de la vidéosurveillance, sur le même traitement de données dont elle aura été saisi auparavant sur base de l'article 27 précité.

Enfin, dans l'hypothèse où la commission consultative précitée adopterait un avis pour lequel la Commission nationale aurait exprimé son désaccord lors de son analyse, en tant que membre de ladite commission consultative, il y a lieu de relever que la CNPD

pourrait, ultérieurement aussi être amenée, le cas échéant, en tant qu'autorité de contrôle indépendante, à exercer sa mission de contrôle, sans toutefois être liée par l'avis qui aurait été rendu par la commission consultative précitée.

En considération des observations qui précèdent, la CNPD voudrait se rapporter à prudence du gouvernement (s'agissant d'un projet de règlement grand-ducal) et du législateur quant à l'opportunité de prévoir la CNPD comme membre de la commission consultative en question.

Ainsi décidé à Belvaux en date du 7 mai 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 2 mars 2021, Monsieur le Ministre du Logement a saisi la Commission nationale d'une demande d'avis sur le projet de loi n°7763 1. portant introduction d'un fonds de travaux ; 2. modifiant la loi modifiée du 16 mai 1975 portant statut de la copropriété des immeubles bâtis (ci-après le « projet de loi ») et projet de règlement grand-ducal modifiant le règlement grand-ducal prescrivant les mesures d'exécution de la loi du 16 mai 1975 portant statut de la copropriété des immeubles (ci-après le « projet de règlement grand-ducal »).

Il ressort de l'exposé des motifs que le projet de loi vise à instaurer un fonds de travaux obligatoire

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7763 1. portant introduction d'un fonds de travaux ; 2. modifiant la loi modifiée du 16 mai 1975 portant statut de la copropriété des immeubles bâtis et au projet de règlement grand-ducal modifiant le règlement grand-ducal prescrivant les mesures d'exécution de la loi du 16 mai 1975 portant statut de la copropriété des immeubles. (Délibération n°18/AV14/2021 du 14/05/2021)

pour les copropriétés des immeubles bâtis dans le but de promouvoir la rénovation, de façon générale, et plus particulièrement la rénovation énergétique. Ledit fonds de travaux devrait également contribuer à augmenter la conscience des propriétaires quant à la nécessité de constituer une trésorerie suffisante pour faire face aux frais d'entretien et d'optimisation de l'utilisation rationnelle des ressources de leur patrimoine immobilier, sans se limiter à l'effort consenti pour l'acquisition d'un immeuble, ainsi qu'à prévenir, de façon générale, la dégradation et l'insalubrité des immeubles bâtis en copropriété.

Le présent avis se limitera aux questions relatives aux aspects de la protection des données à caractère personnel soulevées par l'article 1^{er} du projet de loi, le projet de règlement grand-ducal ne soulevant pas de questions relatives à la protection des données à caractère personnel.

L'article 1^{er} du projet de loi prévoit l'insertion d'un nouvel article 11 bis dans la loi modifiée du 16 mai 1975 portant statut de la copropriété des immeubles bâtis, qui instaure une obligation dans le chef des copropriétaires de constituer un fonds de travaux pour faire face au coût des travaux décidés par l'assemblée générale.

6

ANNEXES

Ce fonds est alimenté par une cotisation annuelle obligatoire versée par chacun des copropriétaires. Le versement de ces cotisations est attaché aux lots et définitivement acquises au syndicat des copropriétaires. Il ressort de la lecture du commentaire des articles que les cotisations versées au titre du fonds de travaux sont calculées en tenant compte des règles générales de la répartition des charges.

L'article 11 bis nouveau du projet de loi prévoit encore qu'en cas de vente d'un lot par un des copropriétaires, l'acheteur intéressé par l'acquisition de ce lot « *doit pouvoir consulter un extrait reprenant le solde actuel des cotisations au fonds de travaux acquises par ce lot* ». Les auteurs du projet de loi précisent à ce sujet qu'en pratique « *le syndic établira ces extraits et les mettra à disposition des propriétaires, afin qu'ils puissent répondre à leurs obligations légales de consultation et de communication à l'égard des (futurs) acquéreurs et vendeurs* ».

En l'absence de précision sur le contenu d'un tel extrait dans le commentaire des articles et dans le projet de loi, la CNPD comprend, toutefois, que des données à caractère personnel seraient susceptibles de figurer sur un tel document, notamment des données à caractère personnel relatives au copropriétaire mettant en vente son lot.

Dès lors, il y a lieu de féliciter les auteurs du projet de loi d'avoir prévu une base légale en vertu de laquelle le syndic établira cet extrait pour le mettre à disposition du copropriétaire afin que celui-ci réponde à son obligation légale de consultation et de communication à l'égard des futurs acquéreurs et vendeurs.

Enfin, la Commission nationale profite de l'opportunité, suite à sa saisie, de faire part d'une problématique à laquelle elle a été confrontée dans le cadre du traitement de demandes d'informations et de réclamations, qui concernent la transparence des informations communiquées par le syndic aux copropriétaires. A cet égard, il pourrait être utile de préciser dans les dispositions du règlement grand-ducal du 13 juin 1975 prescrivant les mesures d'exécution de la loi du 16 mai 1975 portant statut de la copropriété des immeubles, et en particulier dans son article 5, si et dans quelles conditions la transmission par le syndic de la situation comptable individuelle détaillée d'un copropriétaire aux autres copropriétaires (respectivement aux membres du conseil de copropriété) est possible. En effet, en dehors d'une telle disposition légale, la Commission nationale ne voit pas quelle autre condition de licéité au sens de l'article 6 du RGPD aurait vocation à légitimer une telle transmission de données par le syndic à des tiers.

Ainsi décidé à Belvaux en date du 14 mai 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7787 relatif à la mise en œuvre du règlement (UE) 2017/821 du Parlement européen et du Conseil du 17 mai 2017 fixant des obligations liées au devoir de diligence à l'égard de la chaîne d'approvisionnement pour les importateurs de l'Union qui importent de l'étain, du tantale et du tungstène, leurs minerais et de l'or provenant de zones de conflit ou à haut risque. (Délibération n°19/AV/15/2021 du 14/05/2021)

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 18 mars 2021, Monsieur le Ministre des Affaires étrangères et européennes a saisi la Commission nationale d'une demande d'avis sur le projet de loi n°7787 relatif à la mise en œuvre du règlement (UE) 2017/821 du Parlement européen et du Conseil du 17 mai 2017 fixant des obligations liées au devoir de diligence à l'égard de la chaîne d'approvisionnement pour les importateurs de l'Union qui importent de l'étain, du tantale et du tungstène, leurs minerais et de l'or provenant de zones de conflit ou à haut risque (ci-après le « projet de loi »).

Il ressort de l'exposé des motifs que l'objectif du projet de loi est de prendre au niveau national les mesures nécessaires pour la mise en œuvre du règlement (UE) 2017/821 précité, lequel vise à

endiguer le commerce de l'étain, du tantale et du tungstène, leurs minerais et de l'or (ci-après les « 3TG ») provenant de zones de conflit ou à haut risque en imposant aux importateurs de l'Union européenne un certain nombre d'obligations. Plus concrètement, les entreprises tombant sous le champ d'application du règlement (UE) 2017/821 sont donc incitées à faire le nécessaire pour que les 3TG importés au Luxembourg ne proviennent pas de zones de conflit.

Le présent avis se limitera aux questions relatives aux aspects de la protection des données à caractère personnel soulevées par les articles 5 à 8 du projet de loi.

Or, il ne ressort pas clairement de ces articles quels traitements de données seraient mis en œuvre par le ministre ayant les Affaires étrangères dans ses attributions (ci-après « l'autorité compétente ») et par l'Administration des douanes et accises, ou quelles seraient les catégories de données à caractère personnel qui seraient, le cas échéant, collectées par l'autorité compétente et par l'Administration des douanes et accises.

Ainsi, l'article 5 du projet de loi liste les « renseignements » qui pourraient être fournis à l'autorité compétente et à l'Administration des douanes et accises. Cependant, il est difficile pour la Commission nationale de savoir si des données à caractère personnel seraient

6

ANNEXES

effectivement contenues dans ces renseignements. Rappelons que l'article 4 numéro (1) du RGPD définit la notion de donnée à caractère personnel comme « (...) toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Dans ce contexte, elle comprend que « les noms des personnes en charge de la supervision du processus interne selon l'article 4, lettre c), du règlement (UE) 2017/281 », visés à l'article 5, paragraphe (2), numéro 2 du projet de loi pourraient effectivement constituer des données à caractère personnel au sens du RGPD.

Les articles 6 et 7 du projet de loi portent quant à eux sur des échanges d'informations, entre l'Administration des douanes et accises et l'autorité compétente (article 6), et avec la Commission européenne et les autorités compétentes des autres Etats membres (article 7), sans qu'il ne ressorte précisément de ces articles si ces informations comporteraient ou non des données à caractère personnel.

Enfin, l'article 8 du projet de loi se limite à indiquer que l'autorité compétente et l'Administration des douanes et accises ont la qualité de « responsables conjoints du traitement des données », sans toutefois préciser les traitements de données y relatifs. Relevons à ce sujet que l'article 26 du RGPD prévoit que

les responsables conjoints du traitement des données « définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du [RGPD], notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'Etat membre auquel les responsables du traitement sont soumis ». La Commission nationale se permet par ailleurs de relever une petite erreur matérielle : il conviendrait d'ajouter le terme « du » entre « l'article 26 » et « règlement ».

Compte tenu des développements qui précèdent, la Commission nationale rappelle que la définition de responsables du traitement conjoints dans cet article 8 ne serait pertinente que sous condition que des données à caractère personnel sont effectivement traitées.

Ainsi décidé à Belvaux en date du 14 mai 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

Avis de la Commission nationale pour la protection des données relatif à la proposition de loi n°7808 relative à la stratégie de dépistage du virus Covid-19 dans les structures pour personnes vulnérables et dans les réseaux d'aides et de soins.

(Délibération n°20/AV16/2021 du 28/05/2021)

Conformément à l'article 57, paragraphe 1^{er}, lettre (c) du règlement (UE) 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 1^{er} 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 19 mai 2021, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur la proposition de loi n°7808 de Monsieur le Député Michel Wolter relative à la stratégie de dépistage du virus Covid-19 dans les structures pour personnes vulnérables et dans les réseaux d'aides et de soins (ci-après la « proposition de loi »). Dans la mesure où des amendements ont été adoptés par la Commission de la Santé et des Sports en date du 19 mai 2021, le présent avis portera sur la proposition de loi, telle qu'amendée.

La proposition de loi a pour objet de rendre obligatoire la réalisation de tests

autodiagnostiques servant au dépistage du SARS-CoV-2 pour les membres du personnel²¹⁸, les prestataires de services externe²¹⁹ ainsi que les visiteurs âgés de six ans et plus²²⁰, avant l'entrée dans l'une des structures visées à l'article 1 du texte sous avis, à moins qu'ils puissent présenter un résultat négatif d'un test d'amplification génique du virus SARS-CoV-2 datant de moins de soixante-douze heures ou d'un test antigénique rapide SARS-CoV-2 certifié datant de moins de vingt-quatre heures²²¹.

L'article 6 de la proposition de loi précise que sont exemptes de ces obligations, les personnes précitées qui sont en mesure de présenter un certificat de vaccination Covid-19 valable ou un certificat de test de dépistage sérologique prouvant la présence d'anticorps anti-coronavirus dans le sang reconnu par la Direction de la santé.

A titre de remarque liminaire, la Commission nationale se demande pourquoi de telles obligations seraient instaurées uniquement dans le chef desdites structures alors que des obligations similaires ne semblent pas être prévues, à l'heure actuelle, pour d'autres organismes, hormis les établissements de restauration, de débit de boissons, d'hébergement, les cantines et les restaurants sociaux²²².

²¹⁸ Article 4 de la proposition de loi, telle qu'amendée

²¹⁹ Article 5 de la proposition de loi, telle qu'amendée

²²⁰ Article 3 de la proposition de loi, telle qu'amendée

²²¹ Articles 3 à 5 de la proposition de loi, telle qu'amendée

²²² Voir Chapitre 1bis de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19.

6

ANNEXES

De plus, il ne ressort pas clairement de la proposition de loi, ni du commentaire des articles, si des traitements de données à caractère personnel seraient effectués par l'employeur ou l'exploitant d'une des structures, visées à l'article 1 de la proposition de loi, suite à la présentation par un visiteur, un employé ou un prestataire de service externe, du résultat négatif ou positif du test antigénique rapide ou du test Covid-19 PCR, d'un certificat de vaccination ou d'un certificat de test de dépistage sérologique prouvant la présence d'anticorps anti-coronavirus dans le sang²²³.

L'employeur ou l'exploitant collectera-t-il ou enregistrera-t-il les données figurant sur lesdits tests ou lesdits certificats suite à leur présentation ?

A cet égard, il y a lieu de rappeler que le RGPD n'aura vocation à s'appliquer que lorsqu'un traitement de données à caractère personnel sera effectué, par exemple si le fait qu'un employé ou visiteur a présenté un résultat de test antigénique rapide, un certificat de vaccination ou un certificat de test de dépistage sérologique est amené à être consigné par l'organisme. En effet, conformément à l'article 2 paragraphe (1) du RGPD « *[l]e présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* ». De plus, l'article 4 paragraphe (2) du RGPD définit le traitement comme « *toute opération ou tout ensemble*

d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

Par ailleurs, bien que ces problématiques ne relèvent pas du domaine de la protection des données, la CNPD s'interroge, en termes de droit du travail, sur les conséquences d'un refus par un employé ou un prestataire de service externe de se soumettre à de telles obligations. L'employé devra-t-il travailler à un autre poste ? Quelles seront les conséquences pour un prestataire de service externe alors que la structure n'est pas son employeur ?

En outre, dans l'hypothèse où des traitements de données seraient effectués dans le cadre de la proposition de loi, ceux-ci doivent reposer sur une des bases de licéité énumérée à l'article 6 du RGPD ainsi que respecter l'une des conditions visées à l'article 9, paragraphe (2), du RGPD dans la mesure où des données relatives à la santé des personnes concernées seraient susceptibles d'être traitées.

A ce titre, il y a lieu de rappeler que le traitement de données à caractère personnel collectées et traitées en vertu d'une obligation légale doit reposer sur une base légale conformément

²²³ Article 7 de la proposition de loi, telle qu'amendée dispose que « *[l]e résultat du test antigénique rapide ou du test Covid-19 PCR, le certificat de vaccination ou le certificat de test de dépistage sérologique prouvant la présence d'anticorps anti-coronavirus dans le sang sont à présenter à l'employeur ou à l'exploitant de la structure sur simple demande.* ».

à l'article 6, paragraphe (3), du RGPD, lu ensemble avec son paragraphe (1), lettres c). Conformément à l'article 6, paragraphe (3), du RGPD cette obligation légale devrait définir les finalités du traitement et 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* ».

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'homme²²⁴.

Or, force est de constater que si des traitements de données devaient être effectués sur base de la proposition de loi, ceux-ci ne pourraient valablement reposer sur une telle base de licéité alors que le dispositif sous avis ne respecte pas les exigences exposées ci-avant.

Enfin, il y a encore lieu de s'interroger sur ce qu'il adviendra lorsque l'employeur ou la structure pour personne vulnérable sera confrontée à une personne lui présentant un test positif.

A ce sujet, l'article 8 de la proposition de loi dispose que « *[t]out test autodiagnostique servant au dépistage du SARS-CoV-2 positif d'une des personnes mentionnées dans les articles 3 à 5 nécessite un auto-isolement immédiat de la personne qui s'est testée et une déclaration par la personne à l'inspection sanitaire de la Direction de la Santé. La procédure et les modalités pratiques de l'auto-déclaration en cas de résultat de test positif par la personne qui s'est testée elle-même sont définies par voie de règlement grand-ducal.* ».

La Commission nationale comprend dès lors que la transmission de données de santé dans ce cadre serait directement effectuée par la personne concernée à l'inspection de la Direction de la Santé, de sorte qu'aucun traitement de données ne serait mis en œuvre par les structures pour personnes vulnérables ou les employeurs.

Néanmoins, dans la mesure où la CNPD n'est pas en possession du projet de règlement grand-ducal qui aurait pour objet de définir la procédure et les modalités pratiques de l'auto-déclaration en cas de résultat de test positif par la personne qui s'est testée elle-même, celle-ci ne peut se prononcer plus en détails à ce sujet.

²²⁴ 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. Voir entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015, CourEDH, Vavříčka et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.

6

ANNEXES

En conclusion, en considération des observations qui précèdent, la Commission nationale considère que dans l'hypothèse où des traitements de données seraient effectués par les organismes concernés, le texte sous avis ne respecterait 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'homme²²⁵, et ne peut, dès lors, se prononcer plus en détail sur les éventuels aspects qui seraient liés à la protection des données personnelles.

Ainsi décidé à Belvaux en date du 28 mai 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

²²⁵ 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, CourEDH, Vavříčka et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.

**Avis de la Commission nationale pour la protection
des données relatif à la proposition de loi n°7797
portant modification de la loi modifiée du 17 juillet 2020
sur les mesures de lutte contre la pandémie Covid-19.
(Délibération n° 21/AV17/2021 du 28/05/2021)**

Conformément à l'article 57, paragraphe 1^{er}, lettre (c) du règlement (UE) 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 1^{er} 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 19 mai 2021, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur la proposition de loi n°7797 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 (ci-après la « proposition de loi »).

Selon l'exposé des motifs, la proposition de loi a pour objet d'obliger les organismes gestionnaires des structures d'hébergement pour personnes âgées et les exploitants des réseaux d'aides et de soins actifs dans le domaine du logement encadré pour personnes âgées, à mettre en place un protocole sanitaire à accepter par la Direction de la Santé.

La Commission nationale considère que la proposition de loi ne soulève pas de question particulière d'un point de vue de la protection des données, dans la mesure où aucun traitement de données à caractère personnel n'a pu *a priori* être identifié dans le texte de la proposition sous avis.

En effet, en l'absence de précisions quant aux modalités du protocole sanitaire qui serait mis en place par les organismes gestionnaires des structures d'hébergement pour personnes âgées et les exploitants des réseaux d'aides et de soins actifs dans le domaine du logement encadré pour personnes âgées, la CNPD n'est pas en mesure d'apprécier si un tel protocole impliquerait des traitements de données à caractère personnel.

Ainsi décidé à Belvaux en date du 28 mai 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal prescrivant un recensement général de la population, des logements et des bâtiments du Grand-Duché au 1^{er} juin 2021 et amendements gouvernementaux. (Délibération n°23/AV18/2021 du 1^{er} juin 2021)

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 2 avril 2021, Monsieur le Ministre de l'Economie a invité la Commission nationale à aviser le projet de règlement grand-ducal prescrivant un recensement général de la population, des logements et des bâtiments du Grand-Duché au 1^{er} juin 2021 (ci-après le « projet de règlement grand-ducal ») ainsi que

des amendements gouvernementaux au projet de règlement grand-ducal, adoptés par le Conseil de gouvernement dans sa séance du 2 avril 2021 (ci-après les « amendements »).

Le projet de règlement a pour objet l'organisation du recensement général de la population, des logements et des bâtiments, qui aura lieu le 8 novembre 2021. Ce recensement sera organisé et dirigé par l'Institut national de la statistique et des études économiques du Grand-Duché de Luxembourg (ci-après le « STATEC ») conformément à l'article 2 de la loi modifiée du 10 juillet 2011 portant organisation de l'Institut national de la statistique et des études économiques et modifiant la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat (ci-après la « loi modifiée du 10 juillet 2011 portant organisation du STATEC » ou la « loi organique du STATEC »), qui dispose que le STATEC a pour mission « *de réaliser les recensements de la population, du logement et des bâtiments, la date et les modalités de ces recensements étant fixées par règlement grand-ducal* ».

De plus, il ressort de l'exposé des motifs que « *[l]a réalisation de cette opération statistique tombe sous le règlement (CE) N° 763/2008 du Parlement Européen et du Conseil du 9 juillet 2008 concernant les recensements de la population et du logement qui a pour objet d'établir « des règles communes pour la fourniture décennale de données exhaustives sur la population et le logement* ». Les auteurs du projet de loi précisent encore qu'au niveau national, l'article 4bis de la loi communale modifiée du 13 décembre 1988 dispose qu'« *[e]*

n vue de déterminer le nombre des membres du conseil communal assignés à chaque commune, il est procédé, au moins tous les dix ans, au recensement de la population du Grand-Duché de Luxembourg. La date et les modalités de ce recensement sont fixées par règlement grand-ducal (...).

Le projet de règlement grand-ducal repose dès lors sur lesdites législations.

Par ailleurs, il ressort de l'exposé des motifs que la nouveauté de ce prochain recensement sera le recours par le STATEC à un recensement dit « combiné ». Les auteurs du projet de règlement grand-ducal précisent que le recensement combiné reposera sur l'accès, par le STATEC, à des données contenues dans des registres administratifs et sur des données collectées à travers des questionnaires en version papier et en version électronique. Ce recensement « combiné » se distinguera des autres recensements effectués par le passé, qui se faisaient sur base des données collectées via un questionnaire en version papier.

Il est, dès lors, indéniable que le recensement qui sera prochainement effectué par le STATEC soulève des problématiques ayant trait à la protection des données pour lesquelles la Commission nationale formulera les observations ci-après.

I. Remarques liminaires

Tout d'abord, il y a lieu de relever que l'article 11, paragraphe (3), de la Constitution érige en

matière réservée à la loi les exceptions à la garantie par l'Etat de la protection de la vie privée²²⁶.

De plus, l'article 32, paragraphe (3), de la Constitution dispose que « [d]ans les 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 l'objectif des mesures d'exécution et le cas échéant les conditions auxquelles elles sont soumises ».

Depuis la révision du 18 octobre 2016 dudit article, « la Cour constitutionnelle considère que dans les matières réservées les éléments essentiels sont du domaine de la loi, tandis que les éléments moins essentiels peuvent être relégués à des règlements et arrêtés pris par le Grand-Duc. Elle fait ainsi sienne la position du constituant, partagée par le Conseil d'Etat, qui consiste à assurer au pouvoir exécutif la faculté de régler les détails des matières réservées, les principes et les points essentiels restant du domaine de la loi. D'après le constituant, de simples lois-cadres fixant quelques grands principes et abandonnant l'essentiel des règles de fond et de forme aux règlements d'exécution ne satisfont pas à ces exigences constitutionnelles. Si des éléments essentiels sont du domaine de la loi, les mesures d'exécution, c'est-à-dire des éléments plus techniques et de détails, peuvent être du domaine du pouvoir réglementaire grand-ducal »²²⁷.

Or, force est de constater que tant l'article 2 de la loi modifiée du 10 juillet 2011 portant

²²⁶ Voir en ce sens M. Besch, Normes et légistique en droit public luxembourgeois, Vademecum, Larcier, Edition 2019, p.472, n°619.

²²⁷ Voir M. Besch, Normes et légistique en droit public luxembourgeois, Vademecum, Larcier, Edition 2019, p.37, n°19.

organisation du STATEC que l'article 4bis de la loi communale modifiée du 13 décembre 1988 se bornent à respectivement énoncer que le STATEC a pour mission de « *réaliser les recensements de la population, du logement et des bâtiments, la date et les modalités de ces recensements étant fixées par règlement grand-ducal* » et qu'« *[e]n vue de déterminer le nombre des membres du conseil communal assignés à chaque commune, il est procédé, au moins tous les dix ans, au recensement de la population du Grand-Duché de Luxembourg. La date et les modalités de ce recensement sont fixées par règlement grand-ducal (...)* ».

Ainsi, la Commission nationale se demande si le projet de règlement grand-ducal est susceptible de ne pas être conforme au dispositif constitutionnel précité alors qu'il réglerait des points essentiels d'une matière réservée à la loi, notamment lorsqu'il définit qui est le responsable du traitement, les finalités des traitements qui seraient mis en œuvre, en ce qu'il prévoit l'accès à des fichiers administratifs par le STATEC, ou encore en ce qu'il prévoit l'utilisation du numéro d'identification national « *en vue de l'interconnexion des différents registres administratifs* »²²⁸.

Dès lors, ne faudrait-il pas veiller à une application rigoureuse des principes d'encadrement normatif susmentionnés s'agissant de la distinction entre ce qui doit relever, par essence, de la loi au sens stricte et ce qui peut faire l'objet d'un encadrement normatif par un texte réglementaire ?

Par conséquent, la CNPD estime que le rôle des différents acteurs impliqués dans le recensement, les finalités du traitement, le principe de l'accès par le STATEC à des registres administratifs dans le cadre du recensement ou encore l'utilisation du numéro d'identification national devraient être prévus dans la loi au sens stricte du terme, et non pas dans un acte réglementaire²²⁹.

II. Sur les traitements de données à des fins statistiques

Il y a lieu de relever que l'article 2 du projet de règlement grand-ducal énumère les données qui seraient collectées à des fins statistiques.

La CNPD formulera, ci-après, ses observations en ce qui concerne les problématiques ayant trait à la protection des données et qui sont soulevées dans le cadre de tels traitements.

1. Sur la conformité de la loi modifiée du 10 juillet 2011 portant organisation du STATEC aux règles applicables en matière de protection des données

Il y a lieu de relever que la loi modifiée du 10 juillet 2011 portant organisation du STATEC revêt une importance particulière dans le cadre de l'organisation du recensement. Cette loi encadre notamment les pouvoirs dont dispose le STATEC lorsque celui-ci est amené à procéder à des opérations statistiques, tel que cela est le cas dans le cadre du recensement.

²²⁸ Projet de règlement grand-ducal, exposé des motifs, page 5.

²²⁹ Voir en ce sens M. Besch, Normes et légistique en droit public luxembourgeois, Vademecum, Larcier, Edition 2019, p.472, n°619.

Les auteurs du projet de règlement grand-ducal indiquent que les dispositions de l'article 2 de ladite loi « constituerait déjà une base légale suffisante pour réaliser le recensement »²³⁰ et que le STATEC « est habilité par la [loi modifiée du 10 juillet 2011 portant organisation du STATEC] (...) à accéder et à utiliser les sources administratives à des fins statistiques »²³¹ ou encore que l'article 12 de ladite loi « stipule que dans le choix du mode de collecte de données, le STATEC privilégie l'exploitation des fichiers administratifs. Il ne recourt à des enquêtes ou recensements que si l'exploitation des fichiers administratifs s'avère impossible ou n'est pas susceptible de fournir des informations statistiques fiables et pertinentes »²³².

En effet, l'article 12 de la loi modifiée du 10 juillet 2011 portant organisation du STATEC dispose que « dans le choix du mode de collecte de données le STATEC privilégie l'exploitation des fichiers administratifs ». L'article 13 de ladite loi dispose encore que « les administrations publiques, les communes et les établissements publics ainsi que toutes les personnes physiques ou morales sont tenues de fournir les renseignements statistiques demandés par le STATEC dans les délais fixés dans sa requête » et que « dans le cadre des missions prévues à l'article 2, le STATEC a un droit d'accès aux informations, même individuelles, contenues dans les fichiers et bases de données des administrations et services publics, collectées dans le cadre de leurs attributions administratives ».

Cependant, dans la mesure où les dispositions de la loi organique du STATEC sont antérieures

aux dispositions du RGPD, il y a lieu de s'interroger sur la conformité des dispositions de la loi organique du STATEC avec celles de l'article 6, paragraphe (3), du RGPD (i) ainsi que sur l'articulation entre les dispositions de la loi précitée avec celles de l'article 65 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données (ii).

i. Sur l'article 6, paragraphe (3), du RGPD

Comme relevé précédemment, la Commission nationale comprend que les auteurs du projet de règlement grand-ducal entendent faire reposer sur les articles 12 et 13 de la loi modifiée du 10 juillet 2011 portant organisation du STATEC l'accès par le STATEC aux registres administratifs, visés à l'article 3 du projet de règlement grand-ducal.

Cependant, il y a lieu de s'interroger sur la conformité des dispositions précitées avec celles de l'article 6, paragraphe (3), du RGPD.

En effet, il y a lieu de rappeler que 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

²³⁰ Projet de règlement grand-ducal, exposé des motifs, page 7.

²³¹ Projet de règlement grand-ducal, Ad article 3.

²³² Projet de règlement grand-ducal, exposé des motifs, page 7.

6

ANNEXES

l'Union européenne, soit par le droit de l'Etat 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 Etat 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'homme²³³.

De plus, il ressort de l'ouvrage intitulé « Normes et légistique en droit public luxembourgeois » que cette jurisprudence « exige encore que la base en droit interne soit accessible à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit. Pour satisfaire à l'exigence de prévisibilité, il

s'impose que la « loi », dans son acception matérielle, use 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, en l'occurrence l'ingérence dans la vie privée protégée par l'article 8 de la Convention européenne des droits de l'homme»²³⁴.

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 missions²³⁵. 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 »²³⁶.

Or, force est de constater que les dispositions des articles 12 et 13 de la loi modifiée du 10 juillet 2011 portant organisation du STATEC ne semblent pas remplir les exigences des dispositions précitées notamment en ce qu'elles ne respectent pas les critères de précision et de clarté auxquels doit répondre un texte de loi.

- ii. Sur l'articulation des dispositions de la loi organique du STATEC avec celles de l'article 65 de la loi du 1^{er} août 2018 portant organisation de la Commis-

²³³ En ce sens, voir M. Besch, Normes et légistique en droit public luxembourgeois, Vademecum, Larcier, Edition 2019, p.470, n°619, voir entre autres CourEDH, Zakharov c. Russie [GC], n°47413/06, § 228-229, 4 décembre 2015.

²³⁴ Voir M. Besch, Normes et légistique en droit public luxembourgeois, Vademecum, Larcier, Edition 2019, p.469, n°619.

²³⁵ M. Besch, Normes et légistique en droit public luxembourgeois, Vademecum, Larcier, Edition 2019, p.470, n°619.

²³⁶ M. Besch, Normes et légistique en droit public luxembourgeois, Vademecum, Larcier, Edition 2019, p.470, n°619.

sion nationale pour la protection des données et du régime général sur la protection des données

Comme relevé précédemment, la loi organique du STATEC est antérieure au RGPD ainsi qu'à l'entrée en vigueur de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. Or, ces deux derniers textes légaux prévoient des mesures spécifiques quant au traitement de données à des fins statistiques.

En effet, conformément à l'article 89 du RGPD, le traitement de données à caractère personnel à des fins statistiques est soumis à « des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties garantissent la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données ».

En ce qui concerne les garanties devant être mises en œuvre par le responsable du traitement, le considérant 156 du RGPD énonce que « [l]es États membres devraient prévoir des garanties appropriées pour le traitement de données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Les États membres devraient être autorisés à prévoir, dans des conditions spécifiques et moyennant des garanties appropriées pour les personnes

concernées, des dispositions particulières et des dérogations concernant les exigences en matière d'information et les droits à la rectification, à l'effacement, à l'oubli, à la limitation du traitement, à la portabilité des données et le droit d'opposition lorsque les données à caractère personnel sont traitées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Les conditions et garanties en question peuvent comporter des procédures spécifiques permettant aux personnes concernées d'exercer ces droits si cela est approprié eu égard aux finalités du traitement spécifique concerné, ainsi que des mesures techniques et organisationnelles visant à réduire à un minimum le traitement des données à caractère personnel conformément aux principes de proportionnalité et de nécessité ».

En ce qui concerne plus particulièrement les traitements à des fins statistiques, le considérant 162 du RGPD apporte les précisions suivantes « [l]orsque des données à caractère personnel sont traitées à des fins statistiques, le présent règlement devrait s'appliquer à ce traitement. Le droit de l'Union ou le droit des États membres devrait, dans les limites du présent règlement, déterminer le contenu statistique, définir le contrôle de l'accès aux données et arrêter des dispositions particulières pour le traitement de données à caractère personnel à des fins statistiques ainsi que des mesures appropriées pour la sauvegarde des droits et libertés de la personne concernée et pour préserver le secret statistique. ».

6

ANNEXES

En droit luxembourgeois, l'article 89 du RGPD est transposé à l'article 65 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données qui énumère les mesures appropriées additionnelles qui doivent être mises en œuvre lors de tels traitements.

Ainsi, au vu de ce qui précède, la CNPD se demande dans quelle mesure les dispositions du chapitre 2 de la loi du 1^{er} août 2018 précitée doivent s'articuler avec les dispositions de la loi modifiée du 10 juillet 2011 portant organisation du STATEC.

2. Sur le rôle des différents acteurs impliqués dans le recensement

Il ressort du projet de règlement grand-ducal que différents acteurs seront impliqués dans le recensement à savoir le STATEC (i), les communes et les agents recenseurs (ii) et le CTIE (iii).

En l'absence de dispositions précises dans le texte sous avis, il convient d'analyser leur rôle d'un point de vue de la protection des données, c'est-à-dire déterminer si les différents acteurs précités agissent en tant que responsable du traitement ou sous-traitant.

i. Sur le rôle du STATEC

L'article 2 de la loi modifiée du 10 juillet 2011 portant organisation du STATEC dispose que

le STATEC a pour mission de « réaliser les recensements de la population, du logement et des bâtiments, la date et les modalités de ces recensements étant fixées par règlement grand-ducal ». L'article 10 du projet de règlement grand-ducal précise encore que « [l]e recensement est organisé, dirigé, dépouillé et contrôlé par le STATEC » et l'article 16 du projet de règlement grand-ducal indique que « [l]es administrations communales et les agents recenseurs se conforment aux circulaires et aux instructions émises par le STATEC concernant l'exécution du présent règlement ».

Le STATEC serait ainsi à qualifier de responsable du traitement au sens de l'article 4, point 7), du RGPD, en ce qu'il détermine les finalités et les moyens du traitement qui serait mis en œuvre dans le cadre du recensement malgré le fait qu'il reviendrait en réalité au législateur ou au gouvernement de déterminer les finalités et les moyens (voir supra au point II.1.i).

La CNPD regrette que le texte sous avis ne précise pas expressément que le STATEC aurait la qualité de responsable du traitement. De telles précisions mériteraient d'être apportées dans le projet de règlement grand-ducal, pour une meilleure compréhension du texte sous avis.

ii. Sur le rôle des communes et des agents recenseurs

En ce qui concerne le rôle des communes et des agents recenseurs dans le cadre de la mise

en œuvre du recensement, l'article 10 du projet de règlement grand-ducal dispose que « [s]ur le plan communal, le recensement est réalisé par des agents recenseurs sous la direction et la surveillance des collègues des bourgmestres et échevins. Ces derniers désignent les agents recenseurs. Les communes s'assurent du caractère exhaustif du dénombrement sur le terrain ». Cet article précise encore que « [l]es communes s'abstiennent d'ajouter aux questionnaires du STATEC toute autre question sous quelque forme que ce soit ».

Les auteurs du projet de règlement grand-ducal précisent dans le commentaire des articles que « [s]i l'organisation générale, le dépouillement des questionnaires ainsi que la publication des résultats sont du domaine des compétences du STATEC, les opérations de collecte des données sur le terrain nécessitent l'intervention des administrations communales. Les communes seront notamment tenues de vérifier que toutes les personnes ayant leur résidence principale sur leur territoire, et n'ayant pas répondu par voie électronique, soient invitées à participer à ce recensement à travers la distribution d'un questionnaire papier à travers un agent recenseur. Elles ne pourront pas ajouter d'autres questions ou collectes d'informations autres que celles prévues dans le cadre du présent règlement. »²³⁷.

Les auteurs du projet de règlement grand-ducal précisent encore que « c'est aux communes de recruter des agents recenseurs chargés de la distribution et de la collecte des questionnaires papier. Il incombe également aux administra-

tions communales de contrôler les documents remis par ces agents recenseurs et de procéder, le cas échéant, aux redressements nécessaires. Les instructions nécessaires sont fournies par des agents du STATEC lors de séances de formation en ligne organisées spécialement à cet effet. A noter que les indemnités des agents recenseurs seront prises en charge par le STATEC »²³⁸.

Enfin, tel qu'énoncé précédemment les communes et les agents recenseurs « se conforment aux circulaires et aux instructions émises par le STATEC concernant l'exécution du présent règlement »²³⁹.

Dans la mesure où les communes agissent sur instructions du STATEC et traitent des données à caractère personnel pour le compte du STATEC, ces dernières seraient à qualifier de sous-traitants au sens de l'article 4, point 8) du RGPD.

Concernant le rôle du sous-traitant, il y a lieu de rappeler que les dispositions de l'article 28 du RGPD seront à respecter et que conformément audit article le sous-traitant « ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement » et « veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ».

La CNPD comprend par ailleurs que les agents recenseurs agiraient sous l'autorité des com-

²³⁷ Projet de règlement grand-ducal, Ad Article 10.

²³⁸ Projet de règlement grand-ducal, exposé des motifs, page 6.

²³⁹ Article 16 du projet de règlement grand-ducal.

6

ANNEXES

munes. Les dispositions de l'article 29 du RGPD²⁴⁰ seraient dès lors également à respecter.

Néanmoins, la CNPD se demande si cette qualification de sous-traitant des communes est susceptible de s'appliquer lorsque celles-ci collectent les documents intitulés « l'état récapitulatif « Quartiers de recensement « QR » »²⁴¹ et « Sections électorales « SE » »²⁴² qui permettent notamment aux communes de certifier le nombre de personnes résidentes par section électorale.

En effet, ces dispositions semblent découler des articles 4bis et 5ter de la loi communale du 13 décembre 1988, telle que modifiée.

Dans son avis du 1^{er} février 2021 relatif au projet de règlement grand-ducal, le Syndicat des Villes et Communes Luxembourgeoises indique d'ailleurs que si « les communes sont fortement impliquées dans la réalisation du recensement général de la population (...) [c]ela s'explique sans doute par le fait que, conformément à l'article 4bis de la loi communale modifiée du 13 décembre 1988, la fixation du nombre des membres des conseils communaux est basée sur le nombre d'habitants déterminés moyennant un recensement décennal ».

Dès lors, pour une meilleure lisibilité du texte sous avis, il serait opportun de clarifier le rôle des communes dans le cadre du recensement afin de permettre de distinguer lorsque celles-ci

collectent des données pour le compte du STATEC ou, le cas échéant, pour leur propre compte.

iii. Sur le rôle du CTIE

Selon l'exposé des motifs, l'une des nouveautés du prochain recensement sera la possibilité de répondre à des questionnaires électroniques via « MyGuichet.lu ». Il ressort du projet de règlement grand-ducal que cette interface numérique a été mise en place par le CTIE en collaboration avec le STATEC²⁴³.

Le CTIE semble dès lors agir en tant que sous-traitant au sens de l'article 4, point 8), du RGPD.

Concernant le rôle du sous-traitant, il y a lieu de rappeler que les dispositions de l'article 28 du RGPD seront à respecter. Conformément audit article le CTIE, en tant que sous-traitant, devra traiter « *les données à caractère personnel que sur instruction documentée du responsable du traitement* » et devra veiller « *à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité* ».

3. Sur la collecte de catégories particulières de données

En vertu de l'article 2 du projet de règlement grand-ducal, le STATEC collectera notamment les informations relatives à « *la situation de famille* »²⁴⁴, « *les liens entre les différents membres du ménage* »²⁴⁵ ou encore « *la situation*

²⁴⁰ L'article 29 du RGPD dispose que « [l]e sous-traitant et toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre. ».

²⁴¹ Article 9, point 5^o, du projet de règlement grand-ducal.

²⁴² Article 9, point 6^o, du projet de règlement grand-ducal.

²⁴³ Article 7 du projet de règlement grand-ducal.

²⁴⁴ Article 2, 1^{er} lettre k) du projet de règlement grand-ducal.

²⁴⁵ Article 2, 1^{er} lettre l) du projet de règlement grand-ducal.

éventuelle de handicap »²⁴⁶. Dans la mesure où ces données sont susceptibles de révéler des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle de la personne recensée, ces données sont à qualifier de catégories particulières de données, dites « données sensibles » au sens de l'article 9 du RGPD.

De tels traitements requièrent une protection spécifique²⁴⁷ 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.

Dans le cas présent, la Commission nationale se demande si le traitement reposera sur l'article 9, paragraphe (2), lettre j), du RGPD qui dispose que « *le traitement est nécessaire 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, 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* », ou 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 ».

En outre, il y a lieu de relever que l'article 64 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données dispose que « *[l]e traitement de catégories particulières de données à caractère personnel telles que définies à l'article 9, paragraphe 1er du [RGPD], peut être mis en œuvre pour les finalités prévues à l'article 9, paragraphe 2, point j) de ce même règlement, si le responsable de traitement remplit les conditions de l'article 65.* ».

L'article 65 de la loi du 1^{er} août 2018 énumère les mesures appropriées additionnelles qui doivent être mises en œuvre par le responsable du traitement lorsque celui-ci est amené à traiter des données à caractère personnel à des fins statistiques.

En l'absence de précisions dans le projet de règlement grand-ducal et dans le commentaire des articles quant aux mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée qui seraient, le cas échéant, prises par le STATEC, la CNPD n'est pas en mesure d'apprécier si les conditions de l'article 9, paragraphe (2), lettre j) ou g), du RGPD seraient remplies en l'espèce.

En ce qui concerne la problématique de l'articulation des dispositions précitées avec

²⁴⁶ Article 2, 1^{er} lettre p) du projet de règlement grand-ducal.

²⁴⁷ 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.

6

ANNEXES

celles du projet de règlement grand-ducal, il est renvoyé *supra* au point II du présent avis.

En tout état de cause, les auteurs du projet de règlement grand-ducal devraient veiller à la bonne cohérence entre l'ensemble des dispositions précitées ainsi que prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

4. Sur la collecte du numéro d'identification national

Il ressort des articles 2, 3, et 4 du projet de règlement grand-ducal que le numéro d'identification national au sens de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques sera collecté lors du recensement à des fins statistiques²⁴⁸ et afin de « *combinaison des différentes sources de données entre elles* »²⁴⁹. Celui-ci serait directement collecté par la STATEC via un accès au Registre National des Personnes Physiques (ci-après le « RNPP »).

Si la Commission nationale comprend que le numéro d'identification national serait nécessaire à la qualité des statistiques réalisées dans le cadre du recensement, il y a toutefois lieu de relever que la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques encadrant l'utilisation du numéro d'identification nationale ne prévoit pas un tel traitement de données.

En effet, l'article 2, paragraphe (2), de la loi précitée dispose que « *[l]es actes, documents*

et fichiers établis visés à l'article 1^{er}, paragraphe (1), lettre b) peuvent contenir le numéro d'identification, à condition que celui-ci soit réservé à l'usage à des fins administratives internes, aux relations entre l'Etat et les communes ou aux relations avec le titulaire du numéro ».

Or, le projet de règlement grand-ducal prévoit que le numéro d'identification national serait traité par le STATEC à des fins statistiques et non à des fins administratives internes, tel que cela est prévu par l'article 2 précité.

Enfin, la CNPD estime que l'utilisation du numéro d'identification national dans le cadre du recensement devrait être encadrée par une loi (voir *supra* points I et II).

5. Sur l'accès aux registres administratifs

Il y a lieu de féliciter les auteurs du projet de règlement grand-ducal sur les précisions apportées par l'article 3 du projet de règlement grand-ducal quant à l'origine des données à caractère personnel. Ledit article dispose, en effet, que « *[l]e recensement se base sur des données issues de registres administratifs ainsi que celles récoltées à travers des questionnaires qui seront fusionnées* ».

Cet article précise encore que lorsque les données ne sont pas collectées via les registres administratifs, le reste des informations, visées à l'article 2 du projet de règlement grand-ducal, seront collectées à l'aide du questionnaire

²⁴⁸ Article 2 du projet de règlement grand-ducal.

²⁴⁹ Article 4 du projet de règlement grand-ducal.

« ménage privé » ou à l'aide du questionnaire « ménage collectif ». Ces questionnaires seront disponibles en version électronique ou en version papier.

Bien qu'il convienne de saluer les précisions apportées par l'article 3 du projet de règlement grand-ducal quant aux catégories de données qui seraient collectées via ces fichiers, la Commission nationale tient à apporter les considérations ci-après.

i. Sur l'accès au RNPP

Il y a lieu de relever que l'article 4, paragraphe (1), de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques dispose qu'« [i]l est établi un registre national qui a pour finalités : (...) la mise à disposition de données de personnes physiques aux responsables des fichiers des organismes publics dans les limites des missions légales de ces organismes ou, à condition que les données soient anonymisées, à des fins statistiques ».

Des précisions quant à la portée de ces dispositions sont apportées par le projet de loi n°6330 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques, duquel il ressort que le « *registre permettra également d'établir des statistiques au sujet de la population au Luxembourg* »²⁵⁰.

Par ailleurs, l'article 41 de la loi modifiée du 19 juin 2013 relative à l'identification des

personnes physiques dispose que « [l]es données ou listes de données figurant au registre national ou communal ne peuvent être communiquées à des tiers. Cette interdiction ne vise pas les autorités, administrations, services, institutions ou organismes habilités, par ou en vertu de la loi, à obtenir de telles données ou listes de données et ce pour les informations sur lesquelles porte cette habilitation ».

La Commission nationale se félicite que de telles précisions soient apportées, ce d'autant plus que les dispositions prévues par l'article 13 de la loi modifiée du 10 juillet 2011 portant organisation du STATEC²⁵¹ sont rédigées de manière vague (voir supra au point II du présent avis).

ii. Sur les registres du Centre commun de la sécurité sociale et des Bâtiments et des Logements

Il ressort de l'article 3 du projet de règlement grand-ducal que le STATEC aura accès au registre du Centre commun de la sécurité sociale et au registre des Bâtiments et des Logements. S'il y a lieu de féliciter les auteurs du projet de règlement grand-ducal pour avoir précisé les catégories de données qui seraient collectées à travers de tels registres, certaines précisions mériteraient d'être apportées.

En effet, il ne ressort pas clairement des dispositions sous avis si le STATEC aura un accès direct au registre du Centre commun de la sécurité sociale dans la mesure où

²⁵⁰ Projet de loi n°6330, document parlementaire n°6330/00, Ad Article 4, page 23.

²⁵¹ L'article 13 de la loi modifiée du 10 juillet 2011 portant organisation du STATEC dispose que le « STATEC a un droit d'accès aux informations individuelles, contenues dans les fichiers et bases de données des administrations et services publics, collectées dans le cadre de leurs attributions administratives ».

6

ANNEXES

l'article 3 du projet de règlement grand-ducal dispose que les données seront « *reprises du Centre commun de la sécurité sociale à travers l'Inspection générale de la sécurité sociale* ».

Aucune précision quant à cet accès n'est cependant apporté par les auteurs du projet de règlement grand-ducal dans le commentaire des articles. S'agit-il, dès lors, d'un accès par le STATEC au registre du Centre commun de la sécurité sociale ou d'une communication de données par l'Inspection générale de la sécurité sociale au STATEC ?

Les auteurs du projet de règlement grand-ducal devraient apporter des précisions à ce sujet.

En ce qui concerne le registre des Bâtiments et des Logements, il y a lieu de relever qu'il ressort de l'exposé des motifs que ce registre a été « *créé et maintenu par le STATEC sur base du recensement de 2011* ». La Commission nationale comprend que le STATEC accèderait donc à un de ses propres fichiers.

A ce titre, il convient de rappeler 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. La CNPD renvoie à ce sujet à ses développements supra au point II du présent avis.

Enfin, si des fichiers devaient être créés par le STATEC, à l'instar du registre des Bâtiments et des Logements, sur base des données collectées dans le cadre du projet de

règlement grand-ducal alors cela devrait être expressément reflété dans le projet de règlement grand-ducal sous avis.

iii. Remarques finales

Il y a lieu de relever que dans son avis du 9 mars 2021 relatif au projet de règlement grand-ducal, le STATEC précise qu'il « *poursuivra, dans les prochaines années, ses efforts afin de récolter un maximum d'informations à travers les registres administratifs et ce afin de réduire la charge statistique des personnes recensées* »²⁵².

Si telle est la volonté du STATEC, il est impératif que des dispositions spécifiques quant aux accès qui seraient prévus à divers registres administratifs soient conformes aux dispositions légales actuelles applicables en matière de protection des données, comme relevé dans les développements supra au point II du présent avis.

6. Sur les mesures de sécurité

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)* ».

L'article 32 du RGPD dispose encore que « *le*

²⁵² Page 5 sous le point 3 intitulé « *Recours aux registres administratifs* ».

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, des fuites de données ou des modifications non désirées.

S'il y a lieu de féliciter les auteurs du projet de règlement grand-ducal d'avoir prévu une interdiction aux « *fonctionnaires concernés, aux agents recenseurs ainsi qu'à toute personne collaborant aux travaux de recensement ou en lien avec lesdits travaux, de divulguer, de diffuser ou d'utiliser à d'autres fins et de quelque manière que ce soit les renseignements et données dont ils viennent à connaître dans l'accomplissement de leur mission ou de leur intervention* »²⁵³, il est toutefois essentiel que de telles mesures de sécurité soient mises en œuvre par le STATEC et les administrations dont les données sont accédées dans le cadre de ses accès aux différents fichiers administratifs, prévus à l'article 3 du projet de règlement grand-ducal, afin d'assurer la confidentialité et la sécurité des données.

Dans ce contexte, il est vivement recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début la personne, et à quelles données précises cette personne aurait accès.

Il est d'ailleurs rappelé qu'un tel accès devrait être limité aux personnes ayant besoin d'en connaître dans le cadre de leur fonction. De même que cet accès ne doit pas permettre une

utilisation qui diffère des finalités pour lesquelles ces données sont traitées.

En outre, il est nécessaire de prévoir un système de journalisation des accès. Sur ce point, la CNPD recommande que les données de journalisation soient conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.

La CNPD souligne aussi l'importance d'effectuer pro activement des contrôles en interne. A cet effet, il convient conformément à l'article 32, paragraphe (1), lettre d), du RGPD de mettre en œuvre une procédure « *visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».

En ce qui concerne, le recueil des données via les questionnaires papiers, le STATEC devrait également s'assurer du respect des dispositions précitées lorsque le recueil desdits questionnaire se fait par les communes ou les agents recenseurs.

Enfin, en ce qui concerne les questionnaires électroniques qui seraient accessibles via la plateforme « MyGuichet.lu », le STATEC devrait également veiller à l'ensemble des dispositions de l'article 32 précitées et s'assurer que le CTIE, en tant que sous-traitant, prend toutes les mesures requises en vertu de l'article précité.

7. Sur la durée de conservation des données

²⁵³ Article 17 du projet de règlement grand-ducal.

6

ANNEXES

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. Au-delà, les données doivent être supprimées ou anonymisées.

Le projet de règlement grand-ducal ne précise pas la durée de conservation des données qui seraient collectées à des fins statistiques, ni quels seraient les critères à prendre en compte afin de déterminer une telle durée.

Cependant, il convient de relever que l'article 16 de la loi modifiée du 10 juillet 2011 portant organisation du STATEC dispose que « *[I] orsque l'accomplissement de ses missions ou les finalités statistiques poursuivies exigent l'utilisation de données d'unités statistiques identifiables, le traitement se fait dans le respect des droits et libertés fondamentales des personnes concernées. L'accès à ces données est réservé aux seules personnes chargées d'établir ces statistiques. Dès que l'identification des unités statistiques et tout particulièrement des personnes physiques n'est plus nécessaire dans la chaîne de production des statistiques, les données seront anonymisées* ».

Conformément aux dispositions précitées faut-il dès lors comprendre que les données seront anonymisées dès que celles-ci ne seront plus nécessaires « *dans la chaîne de production des statistiques* »?

En l'absence de précisions à ce sujet dans le projet de règlement grand-ducal et dans le commentaire des articles, la Commission nationale n'est pas en mesure d'apprécier si, en l'occurrence, le principe de durée de conservation limitée des données serait respecté.

8. Sur les droits des personnes concernées

Selon l'article 5, paragraphe (1), lettre (a), du RGPD, les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (principe de licéité, loyauté, transparence).

Ce principe implique notamment que le STATEC devra respecter les dispositions de l'article 13 du RGPD pour les données collectées directement auprès de la personne concernée, sinon celles de l'article 14 du RGPD, lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée elle-même, c'est-à-dire celles collectées notamment via l'accès aux registres administratifs.

En vertu de ces articles, le responsable du traitement devra fournir à la personne concernée des informations au sujet du traitement la concernant, notamment pour garantir un traitement équitable et transparent. Il est précisé que dans le cas de l'article 14 du RGPD, ces informations devront être fournies à la personne concernée au plus tard un mois après que le responsable du traitement ait obtenu les données.

Par ailleurs, l'article 89, paragraphe (2), du RGPD dispose que « *[l]orsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, le droit de l'Union ou le droit d'un État membre peut prévoir des dérogations aux droits visés aux articles 15, 16, 18 et 21, sous réserve des conditions et des garanties visées au paragraphe 1 du présent article, dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités* ».

L'article 63 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données dispose encore que « *[l]orsque les données à caractère personnel sont traitées à des fins de recherche scientifique ou historique, ou à des fins statistiques, le responsable du traitement peut déroger aux droits de la personne concernée prévus aux articles 15, 16, 18 et 21 du [RGPD] dans la mesure où ces droits risquent de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques, sous réserve de mettre en place des mesures appropriées telles que visées à l'article 65* ».

Si les auteurs du projet du règlement grand-ducal entendent déroger aux droits des personnes concernées conformément aux dispositions précitées, cela devrait être précisé obligatoirement dans le texte sous avis.

III. Sur l'utilisation du numéro d'identification national « à des fins de fusion des données issues des registres administratifs et des questionnaires électroniques ou papiers »

L'article 3 du projet de règlement grand-ducal dispose que les données collectées seraient « *combinées entre elles à travers le numéro d'identification et l'adresse de résidence* ». A ce sujet, les auteurs du projet de règlement grand-ducal précisent dans leur commentaire des articles que « *les données tirées des registres et des sources alternatives (questionnaires électroniques ou papiers) sont fusionnées en ayant recours aux numéros d'identification national. Ces fusions sont réalisées de manière automatisée* »²⁵⁴.

Il ressort encore de l'article 4 du projet de règlement grand-ducal que le numéro d'identification national serait collecté afin de « *combiner les différentes sources de données entre elles* »²⁵⁵. Les auteurs du projet de règlement grand-ducal précisent dans le commentaire des articles qu'un tel numéro d'identification national servirait « *à des fins de fusion des données issues des registres administratifs et des questionnaires électroniques ou papiers* »²⁵⁶.

Cependant, il y a lieu de constater que, dans l'exposé des motifs, les auteurs du projet de règlement grand-ducal emploient une terminologie différente et évoquent l'« *utilisation du numéro d'identification national en vue de l'interconnexion des différents registres administratifs* »²⁵⁷.

²⁵⁴ Projet de règlement grand-ducal, Ad Article 3.

²⁵⁵ Article 4 du projet de règlement grand-ducal.

²⁵⁶ Projet de règlement grand-ducal, Ad Article 4.

²⁵⁷ Projet de règlement grand-ducal, exposé des motifs, page 3.

6

ANNEXES

1. Sur la notion « interconnexion »

Or, en ce qui concerne le terme « interconnexion », il y a lieu de rappeler qu'en matière de protection des données le concept d'« interconnexion »²⁵⁸ signifie que les traitements des données sont reliés et peuvent être gérés par les responsables des différents traitements concernés. Toutefois comme cela ne semble pas être le cas en l'espèce, la CNPD comprend que le STATEC souhaite mettre en commun, par des moyens techniques, les données collectées via les registres administratifs et les questionnaires (sous forme papier et électronique).

Pour plus de clarté et afin d'éviter toute confusion, il conviendrait de veiller à utiliser une terminologie uniforme à ce sujet.

2. Sur le lien entre le numéro d'identification national et la « clé recensement »

Comme relevé ci-avant « *les données tirées des registres et des sources alternatives (questionnaires électroniques ou papiers) sont fusionnées en ayant recours aux numéros d'identification national. Ces fusions sont réalisées de manière automatisée* »²⁵⁹.

Cependant, il ressort encore du projet de règlement grand-ducal que « *[l]e rôle des agents recenseurs est essentiel car, en plus de la distribution des questionnaires papiers, il permet d'améliorer le taux de participation et de faire le lien entre les données issues*

des données administratives et des données issues des questionnaires et ce à travers la 'clé recensement', clé unique qui est indiquée par les agents recenseurs sur les listes de contrôles et sur les questionnaires ».

De plus, dans son avis du 9 mars 2021 relatif au projet de règlement grand-ducal, le STATEC indique que « *[l]a fusion des données issues des registres administratifs et des questionnaires sera facilitée car contrairement à l'option « courrier postal », l'agent recenseur doit indiquer sur chaque questionnaire une clé « recensement » unique par personne. Cette clé, permettant la fusion des données administratives et celles issues des questionnaires au niveau de l'individu, sera utilisée en complément du matricule afin que cette fusion des données soit optimale. Cette fusion des données est une étape clé dans la réussite du recensement de la population. Sans cette fusion, les données récoltées ne seront pas exploitables et le STATEC ne pourra satisfaire les obligations de la réglementation européenne* ».

Or, en l'absence de précision quant aux éléments qui constitueraient cette clé « recensement », la Commission nationale se demande quel serait le lien entre cette clé et le numéro d'identification national, qui ont tous deux pour objet de fusionner les données recueillies dans le cadre du recensement.

En outre, cette clé est-elle constituée d'un numéro aléatoire attribué à une personne recensée ou est-elle constituée en partie du numéro d'identification national de la personne recensée ?

²⁵⁸ La version initiale de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, désormais abrogée, définissait à l'article 2, lettre (j) l'interconnexion comme : « *toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement* ».

²⁵⁹ Projet de règlement grand-ducal, Ad Article 3.

Des précisions à ce sujet mériteraient d'être apportées par les auteurs du projet de règlement grand-ducal.

3. 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. Au-delà, les données doivent être supprimées ou anonymisées.

Il y a lieu de relever que l'article 4 du projet de règlement grand-ducal dispose que le numéro d'identification, l'adresse de résidence, le nom et le prénom « *seront supprimées au maximum trois années après la date de recensement* ».

Cependant, l'article 16 de la loi modifiée du 10 juillet 2011 portant organisation du STATEC dispose que « *[l]orsque l'accomplissement de ses missions ou les finalités statistiques poursuivies exigent l'utilisation de données d'unités statistiques identifiables, le traitement se fait dans le respect des droits et libertés fondamentales des personnes concernées. L'accès à ces données est réservé aux seules personnes chargées d'établir ces statistiques. Dès que l'identification des unités statistiques et tout particulièrement des personnes physiques n'est plus nécessaire dans la chaîne de production des statistiques, les données seront anonymisées* ».

La Commission nationale comprend dès lors que les dispositions de l'article 4 du projet

de règlement grand-ducal dérogent aux dispositions de l'article 16 précité.

S'il convient tout d'abord de rappeler qu'un règlement grand-ducal ne peut déroger à une loi, la CNPD s'interroge encore sur les critères qui justifieraient que le numéro d'identification national, l'adresse de résidence, le nom et le prénom soient conservés au maximum trois ans après la date de recensement ?

En l'absence de précisions à ce sujet dans le commentaire des articles, la Commission nationale n'est pas en mesure d'apprécier si, en l'occurrence, le principe de durée de conservation limitée des données serait respecté.

Des précisions à ce sujet mériteraient d'être apportées par les auteurs du projet de règlement grand-ducal.

Ainsi décidé à Belvaux en date du 1^{er} juin 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

**Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7836 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19.
(Délibération n°24/AV19/2021 du 8 juin 2021)**

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 2021, Madame la Ministre de la Santé a saisi la Commission nationale d'une demande d'avis sur le projet de loi n°7836 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 (ci-après le « projet de loi n°7836 »). Des amendements ont été envoyés en date du 8 juin 2021.

Selon l'exposé des motifs, le présent projet de loi vise à proposer de nouveaux assouplissements par rapport aux mesures actuellement applicables sous l'égide de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie et qui trouvent leur fondement dans la situation épidémiologique actuelle et dans l'évolution généralement favorable des indicateurs d'évaluation.

L'article 3 du projet de loi n°7836 entend introduire un système de tests autodiagnostiques obligatoires servant au dépistage du SARS-CoV-2 pour les membres du personnel, les prestataires de services externes et les visiteurs âgés de plus de six ans dans les établissements hospitaliers, ainsi que dans certaines structures et services qui hébergent ou encadrent des personnes âgées ou handicapées. En vertu des paragraphes (1) alinéa 3 et (2) alinéa 3 dudit article 3, les personnes concernées ne peuvent accéder à leur poste de travail, prester des services ou rendre visite à un patient, un pensionnaire ou un usager si le résultat du test autodiagnostique est positif ou si les personnes concernées refusent ou sont dans l'impossibilité de présenter un des certificats requis.

Le commentaire des articles précise que l'article 3 du projet de loi n°7836 s'inspire de la proposition de loi n° 7808 de l'honorable député Michel Wolter. Ainsi, la CNPD tient à renvoyer aux commentaires formulés dans son avis du 28 mai 2021 concernant précisément la proposition de loi n°7808 de Monsieur le Député Michel Wolter relative à la stratégie de dépistage du virus Covid-19 dans les structures

pour personnes vulnérables et dans les réseaux d'aides et de soins.²⁶⁰

La CNPD s'était demandée, entre autres, si des traitements de données à caractère personnel seraient effectués par l'employeur ou l'exploitant d'une des structures et services mentionnés suite à la présentation par un visiteur, un employé ou un prestataire de service externe, du résultat négatif ou positif du test antigénique rapide ou du test Covid-19 PCR, d'un certificat de vaccination ou d'un certificat de test de dépistage sérologique prouvant la présence d'anticorps anti-coronavirus dans le sang.

Cette observation s'inscrit également dans le cadre du « régime Covid Check » défini à l'article 1^{er} point 28 du présent projet de loi n°7836 dans le sens où la CNPD s'interroge si les établissements accueillant un public ou organisant des manifestations ou événements dont l'entrée est exclusivement réservée aux personnes pouvant se prévaloir soit d'un des certificats tels que visés aux articles 3bis, 3ter, 3quater du projet de loi n°7836, soit d'un test autodiagnostique servant au dépistage du virus SARS-CoV-2 réalisé sur place et dont le

résultat est négatif, procèdent à un traitement de données à caractère personnel.

Par ailleurs, bien que ces problématiques ne relèvent pas du domaine de la protection des données, la CNPD s'interrogeait, en termes de droit du travail, sur les conséquences d'un refus par un employé ou un prestataire de service externe de se soumettre à de telles obligations.

Ainsi décidé à Belvaux en date du 8 juin 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

²⁶⁰ Délibération n° 20/AV16/2021 du 28/05/2021 : <https://cnpd.public.lu/fr/decisions-avis/20201/20-AV16-PL7808-depistage-covid19.html>.

6

ANNEXES

**Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal prescrivant un recensement général de la population, des logements et des bâtiments du Grand-Duché au 8 novembre 2021.
(Délibération n°25/AV20/2021 du 2/07/2021.**

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 1^{er} 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* ».

Le 1^{er} juin 2021, la CNPD a avisé le projet de règlement grand-ducal prescrivant un recensement général de la population, des logements et des bâtiments du Grand-Duché au 1^{er} juin 2021 (ci-après le « projet de règlement grand-ducal ») ainsi que des amendements gouvernementaux au projet de règlement

grand-ducal, adoptés par le Conseil de gouvernement dans sa séance du 2 avril 2021.²⁶¹

Par courrier en date du 11 juin 2021, Monsieur le Ministre de l'Economie a invité la Commission nationale à aviser les amendements gouvernementaux, adoptés par le Conseil de gouvernement dans sa séance du 11 juin 2021 (ci-après les « amendements »).

1. Ad Amendement 1

Les auteurs du projet de règlement grand-ducal précisent dans le commentaire de l'article 2, tel que modifié, que le traitement des données visées audit article et qui concernent la vie sexuelle ou l'orientation sexuelle d'une personne physique seront traitées sur base de l'article 9, paragraphe (2), lettre j), du RGPD.

S'il y a lieu de saluer de telles précisions, la CNPD réitère ses observations formulées dans son avis du 1^{er} juin 2021 quant aux mesures appropriées additionnelles qui devront être mises en œuvre par le STATEC lorsque celui-ci est amené à traiter de telles données à des fins statistiques²⁶² ainsi qu'à la problématique relative à l'articulation des dispositions de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, avec celles du projet de règlement grand-ducal²⁶³.

2. Ad Amendement 2

Cet amendement a pour objet d'introduire un nouvel article 3 qui dispose que « *[l]e*

²⁶¹ Avis de la Commission pour la protection des données relatif au projet de règlement grand-ducal prescrivant un recensement général de la population, des logements et des bâtiments du Grand-Duché au 1^{er} juin 2021 ainsi que des amendements gouvernementaux au projet de règlement grand-ducal, délibération n°23/AV18/2021 du 1^{er} juin 2021.

²⁶² Voir point II. 3., page 10.

²⁶³ Voir point III.1., page 5.

recensement récoltera à des fins administratives les informations suivantes :

a) le nom et le prénom ;

b) le numéro d'identification au sens de la loi modifiée du 19 juin 2013 relative à l'identification des personnes.

Ces informations serviront uniquement à combiner les données des registres administratifs ainsi que celles récoltées à travers les questionnaires ».

Dans le commentaire du nouvel article 3, les auteurs du projet de règlement grand-ducal précisent que ces données serviraient « uniquement » à combiner les différents registres administratifs et qu'aucune utilisation statistique de ces données ne serait prévue par le STATEC.

Pour une meilleure compréhension du dispositif sous avis et dans la mesure où le STATEC sera le responsable du traitement, il y aurait lieu de remplacer le terme « recensement » par le « STATEC ».

En ce qui concerne les données énumérées aux points a) et b) de l'article précité, qui seraient désormais collectées à des fins administratives par le STATEC (et non à des fins statistiques), il y a lieu de s'interroger sur le sens de telles finalités.

Il convient de rappeler que les finalités d'un traitement de données à caractère personnel correspondent à l'objectif qui est poursuivi par le responsable du traitement lorsque celui-ci met

en œuvre un tel traitement. En l'espèce, la CNPD comprend que le STATEC collectera de telles données car celles-ci lui seront nécessaires aux fins de la bonne organisation du recensement.

Par ailleurs, l'utilisation du numéro d'identification national « à des fins administratives internes », tel que visé à l'article 2, paragraphe (2), de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, est à comprendre, par exemple, comme l'utilisation par une administration du matricule d'un de ses administrés dans le cadre du traitement de son dossier.

Dès lors, la Commission nationale se demande si la terminologie employée, pour désigner les finalités prévues par le nouvel article 3, reflète les finalités qui seraient effectivement poursuivies par le STATEC dans un tel contexte.

En tout état de cause, la terminologie employée est trop vague et 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'homme²⁶⁴.

En outre, en ce qui concerne l'utilisation du numéro d'identification national, la CNPD réitère ses observations formulées dans son avis du 1^{er} juin 2021 selon lesquelles elle considère qu'à défaut de base légale appropriée dans la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, l'utilisation du numéro d'identification

²⁶⁴ 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, CourEDH, Vavříčka et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.

6

ANNEXES

national dans le cadre du recensement devrait être encadrée par une loi²⁶⁵.

3. Ad Amendement 3

Il y a lieu de féliciter les auteurs du projet de règlement grand-ducal d'avoir modifié l'article 3, alinéa 3, du projet de règlement grand-ducal suite aux observations formulées par la CNPD dans son avis du 1^{er} juin 2021.

De même que la Commission nationale salue les précisions apportées par les auteurs du projet de règlement grand-ducal, selon lesquelles « [l]e STATEC n'aura pas un accès direct au registre du Centre commun. Seules les données mentionnées seront fournies au STATEC par l'Inspection générale de la sécurité sociale ».

4. Ad Amendement 4

Cet amendement a pour objet de modifier l'article 4, dernier alinéa, du projet de règlement grand-ducal en ces termes « [u]ne fois ces deux opérations terminées, ces informations seront supprimées **dès que l'identification des personnes physiques n'est plus nécessaire dans la chaîne de production des statistiques. Cette suppression des données devra être faite endéans les trois années après la date de recensement de sorte qu'aucune donnée nominative ne figure dans le fichier informatique établi sur la base des données du recensement.** ».

Selon les auteurs du projet de règlement grand-ducal, cet amendement tient compte des remarques de la Commission nationale et

« ce afin d'être cohérent avec l'article 16 de la loi modifiée du 10 juillet 2011 portant organisation du STATEC. Les conditions mentionnées dans cet article sont mêmes plus strictes que celles se trouvant dans la loi du STATEC car ces opérations devront être réalisées endéans les trois ans à partir de la date de recensement ».

Bien qu'il convienne de féliciter les auteurs du projet de règlement grand-ducal d'avoir pris en compte les considérations de la CNPD dans son avis du 1^{er} juin dernier, les critères, qui justifieraient que les données soient supprimées endéans le délai de 3 ans, ne sont pas indiqués dans le texte du projet de règlement grand-ducal ou dans les commentaires de l'article.

Dès lors, en l'absence de telles précisions, la Commission nationale n'est pas en mesure d'apprécier si, en l'occurrence, le principe de durée de conservation limitée des données serait respecté.

Pour le surplus et en ce qui concerne la durée de conservation des données traitées à des fins statistiques et non visées par l'article précité, il convient de réitérer les observations formulées par la CNPD dans son avis précité²⁶⁶.

5. Ad Amendement 5

Il y a lieu de saluer les auteurs du projet de règlement grand-ducal d'avoir précisé les éléments qui composent la clé d'identification.

De plus, bien que l'article 9 du projet de règlement grand-ducal, tel que modifié par

²⁶⁵ Voir points I.1., page 2 et II.4., page 12.

²⁶⁶ Voir point II.7., page 16

l'amendement 5, dispose que « *[c]ette clé technique est unique par personne, ne permet pas de retrouver le matricule et n'est utilisée qu'à des fins administratives* », aucune précision quant au lien qui unirait cette clé et le numéro d'identification national n'a été apportée par les auteurs du projet de règlement grand-ducal.

Or, le STATEC dans son avis du 9 mars 2021 relatif au projet de règlement grand-ducal avait indiqué que cette clé permettrait « *la fusion des données administratives et celles issues des questionnaires au niveau de l'individu, sera utilisée en complément du matricule afin que cette fusion des données soit optimale. Cette fusion des données est une étape clé dans la réussite du recensement de la population. Sans cette fusion, les données récoltées ne seront pas exploitables et le STATEC ne pourra satisfaire les obligations de la réglementation européenne* ».

Dès lors, en l'absence de telles précisions, la CNPD n'est pas en mesure de saisir les problématiques éventuelles qui pourraient se poser d'un point de vue de la protection des données.

En outre, dans la mesure où cette clé constituerait un identifiant unique, elle se demande si une telle clé ne serait pas à analyser comme un « nouveau matricule ».

6. Ad Amendement 6

Il y a lieu de féliciter les auteurs du projet de règlement grand-ducal d'avoir expressément

prévu à l'article 10 du projet de règlement grand-ducal que le STATEC aura la qualité de responsable du traitement au sens de l'article 4, point 7), du RGPD.

Néanmoins, des précisions quant aux rôles des communes, des agents recenseurs et du CTIE, n'ont pas été apportées par les auteurs du projet de règlement grand-ducal. Dès lors, la CNPD réitère à ce sujet ses observations formulées dans son avis du 1^{er} juin 2021²⁶⁷.

En outre, cet amendement introduit un nouvel alinéa 4 à l'article 6 du projet de règlement grand-ducal qui précise que les communes profiteront du recensement « *afin de contrôler, par leurs propres moyens, le caractère exhaustif de leur registre de la population* », tout en prévoyant que les données collectées par ces dernières, dans le cadre du recensement, ne pourront pas être utilisées « *pour mettre à jour leur registre de la population* ».

Or, bien que le principe d'une non réutilisation des données collectées par les communes, dans le cadre du recensement, figure désormais à l'article précité, il y a lieu de s'interroger sur les moyens qui permettraient aux communes de contrôler le caractère exhaustif de leur registre de la population, si ce n'est justement par la réutilisation des données que ces dernières collecteront dans le cadre du recensement.

7. Ad Amendement 7

Cet amendement fait suite aux observations de la Commission nationale formulées dans son

²⁶⁷ Voir point II.2., page 7.

6

ANNEXES

avis du 1^{er} juin 2021 et propose l'introduction d'un nouvel article 21 qui a pour objet de préciser les dérogations qui seraient effectuées aux droits des personnes concernées.

Néanmoins, conformément au principe de la hiérarchie des normes juridiques, qui impose le parallélisme des formes, de telles dispositions, qui entendent déroger aux droits des personnes concernées, tel que prévu à l'article 63 de la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, devraient figurer dans une loi et non dans un règlement grand-ducal.

La Commission nationale réitère d'ailleurs l'ensemble de ses observations formulées dans son avis du 1^{er} juin 2021 relatif à ses interrogations quant à la conformité du projet de règlement grand-ducal aux dispositions des articles 11, paragraphe (3) et 32, paragraphe (3) de la Constitution, alors qu'il réglerait des points essentiels d'une matière réservée à

la loi, notamment lorsqu'il définit qui est le responsable du traitement, les finalités des traitements qui seraient mis en œuvre, en ce qu'il prévoit l'accès à des fichiers administratifs par le STATEC, ou encore en ce qu'il prévoit l'utilisation du numéro d'identification national²⁶⁸.

Ainsi décidé à Belvaux en date du 2 juillet 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

²⁶⁸ Voir point I, page 2.

Conformément à l'article 57, paragraphe 1^{er}, lettre (c) du règlement (UE) 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 1^{er} 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* ».

Le 7 décembre 2018, la CNPD a avisé le projet de loi n° 7126 relative aux sanctions administratives communales modifiant 1) le Code pénal, 2) le Code de procédure pénale, et 3) la loi communale modifiée du 13 décembre 1988 (ci-après le « projet de loi »)²⁶⁹.

Par courrier en date du 19 avril 2021, Madame la Ministre de l'Intérieur a invité la Commission nationale à aviser les amendements gouvernementaux au projet de loi, approuvés par le Conseil du gouvernement dans sa séance du 2 avril 2021 (ci-après les « amendements »).

Avis complémentaire de la Commission nationale pour la protection des données relative aux amendements gouvernementaux au projet de loi n°7126 relatif aux sanctions administratives communales et à l'élargissement des compétences des agents municipaux. (Délibération n°26/AV21/2021 du 9 juillet 2021)

Le présent avis se limitera aux questions relatives aux aspects de la protection des données à caractère personnel soulevées par les amendements 6 et 14 au projet de loi.

I) Ad Amendement 6

Bien que l'amendement 6 ne modifie pas le paragraphe (1) de l'article 7 du projet de loi concernant l'accès du fonctionnaire sanctionnateur au registre national des personnes physiques, la CNPD tient à réitérer ses considérations formulées dans son avis du 7 décembre 2018, selon lesquelles « *le fonctionnaire sanctionnateur devrait avoir accès uniquement aux données pertinentes dans le cadre de l'exercice de ses compétences, c'est-à-dire aux données mentionnées dans le fichier des sanctions administratives communales, et non pas aux autres données comprises dans le registre national des personnes physiques (comme, par exemple, les données concernant la famille de la personne concernée)* ».

II) Ad Amendement 14

L'amendement 14 a pour objet de supprimer les dispositions du Chapitre 7 du projet de loi relatif

²⁶⁹ Avis de la Commission nationale pour la protection des données à l'égard du projet de loi n° 7126 relative aux sanctions administratives communales modifiant 1) le Code pénal, 2) le Code de procédure pénale, et 3) la loi communale modifiée du 13 décembre 1988, délibération du n° 490/2018 du 7 décembre 2018.

6

ANNEXES

aux registres des sanctions administratives communales, qui prévoyaient la création de trois fichiers.

En effet, les articles 18 et 19 du Chapitre 7 précité prévoyaient respectivement que le fonctionnaire sanctionnateur tient un « fichier des infractions dont les constats lui sont transmis » et que les communes et la Police grand-ducale tiennent un « fichier des sanctions administratives ».

La suppression des articles précités, par les auteurs du projet de loi, fait suite aux observations formulées par le Conseil d'Etat dans son avis du 28 novembre 2017 ainsi que dans son avis complémentaire du 23 octobre 2018, selon lesquelles il considère que « *la matière est réglée à suffisance par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* »²⁷⁰ et qu'il convient d'omettre les articles 18 et 19 précités.

Or, la CNPD avait, au contraire, dans son avis du 7 décembre 2018, salué que le projet de loi entendait prévoir le principe de la création de tels registres, conformément à l'article 6, paragraphe (3), du RGPD.

A cet égard, 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 RGPD²⁷¹.

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'Etat 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 Etat 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

²⁷⁰ Voir « examen des articles », Article 18, page 13 du document parlementaire n°7126/04, et « examen des amendements », Amendements 21 et 22, page 9 du document parlementaire n°7126/09.

²⁷¹ L'article 6 paragraphe (3) 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'Etat 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. ».

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'homme²⁷².

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.

Dès lors, 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 missions²⁷³. 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* »²⁷⁴.

Ainsi et malgré la suppression des dispositions précitées, la Commission nationale comprend que de tels registres auraient tout de même vocation à être tenus par le fonctionnaire sanctionnateur, les communes et la Police grand-ducale, en tant que responsables du traitement desdits registres.

Dans un souci de sécurité juridique, la CNPD regrette donc que le texte sous avis ne conserve pas de telles dispositions et estime nécessaire que les dispositions des articles 18 et 19 du projet de loi soient conservées, alors qu'elles prévoient la création de tels fichiers. Celles-ci devront, en outre, contenir les éléments cités ci-avant.

Pour le surplus, la CNPD réitère ses observations formulées sous le point II de son avis du 7 décembre 2018.

Ainsi décidé à Belvaux en date du 9 juillet 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

²⁷² 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. Voir entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015, CourEDH, Vavřicka et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.

²⁷³ 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.

²⁷⁴ 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.

6

ANNEXES

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n° 7348 relative aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence et modifiant : 1. la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et 2. la loi modifiée du 7 décembre 2015 sur le secteur des assurances. (Délibération n°27/AV22/2021 du 6 août 2021)

Conformément à l'article 57, paragraphe 1^{er}, lettre (c) du règlement (UE) 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 1^{er} 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 1^{er} février 2019, la CNPD a avisé le projet de loi n° 7348 relative aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence et modifiant : 1. la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance

du secteur financier ; et 2. la loi modifiée du 7 décembre 2015 sur le secteur des assurances (le « projet de loi »)²⁷⁵.

En date du 2 juillet 2021, Monsieur le Directeur du Trésor, pour le compte du Ministre des Finances, a transmis à la CNPD des amendements gouvernementaux au projet de loi pour avis.

La CNPD salue les changements apportés par les amendements 16 et 18, aux articles 28 et 32 du projet de loi, qui précisent dorénavant que les données nécessaires peuvent être collectées par la Caisse de consignation, ce qu'elle avait conseillé dans l'avis précité.

L'amendement 16 vise encore à préciser les modalités de transmission de la demande de consignation à la Caisse de consignation. Suite à l'amendement, les articles 28 et 32 prévoient que la transmission de la demande de consignation ainsi que des informations et pièces supplémentaires doit se faire « *par voie de dépôt électronique sur une plate-forme étatique sécurisée* ». La Commission nationale rappelle qu'en tout état de cause, des mesures de sécurité techniques et organisationnelles appropriées devront être mises en place sur cette plate-forme, conformément à l'article 32 du RGPD.

La CNPD se félicite encore de l'amendement 18, qui vise à préciser le contenu du registre et qui rajoute un paragraphe 6 à l'article 32 disposant que la Caisse de consignation est à considérer comme étant le responsable du traitement au sens de l'article 4. 7) du RGPD des

²⁷⁵ Document parlementaire 7348/02.

traitements mis en œuvre sur base de l'article en question, comme elle l'avait suggéré dans son avis.

Elle regrette cependant que les auteurs des amendements n'ont pas jugé opportun de donner suite aux autres points soulevés par la CNPD, notamment concernant les traitements de données à caractère personnel effectués par les établissements et les entreprises d'assurances, la durée de conservation des données traitées par les responsables de traitement et les transmissions de données aux et entre les organismes publics. Elle réitère dès lors les recommandations faites dans son avis du 1^{er} février 2019.

Ainsi décidé à Belvaux en date du 6 août 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

**Avis complémentaire de la Commission nationale pour la protection des données relatif à l'amendement parlementaire au projet de loi n° 7643 sur les données ouvertes et la réutilisation des informations du secteur public et relatif au projet de règlement grand-ducal portant fixation de critères objectifs, transparents et vérifiables pour calculer le montant total des redevances pour la fourniture et les autorisations de réutilisation des documents détenus par les organismes du secteur public et les entreprises publiques.
(Délibération n° 28/AV23/2021 du 6/08/2021)**

Conformément à l'article 57, paragraphe 1^{er}, 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 (ci-après le « règlement général sur la protection des données » ou le « RGPD »), auquel se réfère l'article 7 de la loi du 1^{er} 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 1^{er} juillet 2021, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer sur l'amendement parlementaire

au projet de loi n° 7643 sur les données ouvertes et la réutilisation des informations du secteur public (ci-après le « projet de loi »), adopté par la Commission de la Digitalisation, des Médias et des Communications de la Chambre des Députés lors de sa réunion du 18 juin 2021.

L'amendement unique vise à introduire un paragraphe 5 à l'article 4 du projet de loi prévoyant la mise en place d'un portail unique regroupant l'ensemble des documents mis à disposition pour des fins de réutilisation afin de répondre à une opposition formelle du Conseil d'Etat. Le commentaire de l'amendement explique encore qu'en plus des « documents disponibles en vue d'une réutilisation », doivent également figurer sur le portail « les conditions éventuelles dont les licences types ainsi que les rétributions éventuelles de cette réutilisation ».

Le commentaire de l'amendement poursuit en indiquant que « [e]n ce qui concerne les autres oppositions formelles émises par le Conseil d'Etat dans son avis du 1^{er} juin 2020 à l'endroit des articles 4, 7 et 12, la Commission de la Digitalisation, des Médias et des Communications a décidé de suivre les propositions de la Haute Corporation.

Le Conseil d'Etat a en outre estimé que l'article 13, paragraphe 2, du projet de loi ne requiert pas de transposition dans la mesure où il a spécifiquement trait aux actes d'exécution qui relèvent de la compétence de la Commission européenne.

La Commission de la Digitalisation, des Médias et des Communications a décidé de suivre l'avis du Conseil d'Etat sur ce point et a, par conséquent, supprimé le paragraphe 2 en question.

Après analyse de l'article 13 modifié, la Commission a toutefois constaté que suite à cette modification, il y a également lieu d'adapter la référence aux paragraphes « 2, 3 et 4 » prévue à l'article 13, paragraphe 1^{er}, point 1^o, pour refléter la nouvelle numérotation des paragraphes subséquents, à savoir « 2 et 3 ».

La Commission nationale rappelle qu'en tout état de cause, les règles applicables en matière de protection des données, et notamment les principes prévus à l'article 5 du RGPD, doivent être respectés dans le cadre de l'exploitation du portail unique.

L'amendement parlementaire ne soulève pas d'autre question particulière d'un point de vue de la protection des données, et renvoie pour le surplus à son avis du 20 janvier 2021.

Ainsi décidé à Belvaux en date du 6 août 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n° 7425 sur les armes et munitions et portant : 1° transposition de la directive (UE) 2021/555 du Parlement européen et du Conseil du 24 mars 2021 relative au contrôle de l'acquisition et de la détention d'armes ; 2° modification du Code pénal, et 3° abrogation de la loi du 20 avril 1881 concernant le transport et le commerce des matières explosives. (Délibération n° 29/AV24/2021 du 1^{er} octobre 2021)

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 1^{er} 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 8 juillet 2019, la CNPD a avisé le projet de loi n°7425 portant : 1° transposition de la directive (UE) 2021/555 du Parlement européen et du Conseil du 24 mars 2021

relative au contrôle de l'acquisition et de la détention d'armes ; 2° modification du Code pénal, et 3° abrogation de la loi du 20 avril 1881 concernant le transport et le commerce des matières explosives (ci-après le « projet de loi »)²⁷⁶.

En date du 4 février 2021, la Commission nationale a rendu son avis complémentaire sur les amendements gouvernementaux adoptés par la Commission de la Justice lors de sa réunion du 27 mai 2020²⁷⁷.

Le 13 juillet 2021, la Commission de la Justice a adopté une série d'amendements parlementaires relative au projet de loi (ci-après les « amendements »).

Dans la mesure où les amendements concernent des articles du projet de loi ayant été commenté par la CNPD et que cette dernière n'a pas été saisie pour avis, elle s'autosaisit afin de faire part de ses observations ci-après.

1. Ad amendement n°22

L'amendement n°22 modifie le paragraphe (1) de l'article 14 du projet de loi, en ce qu'il remplace la notion « honorabilité » par la notion « dangerosité », et insère un nouvel alinéa au paragraphe (3) de l'article 14.

Les auteurs des amendements apportent encore, dans leur commentaire, des précisions quant à certaines interrogations soulevées par le Conseil d'Etat dans son avis complémentaire du 19 décembre 2020.

²⁷⁶ Délibération n°42/2019 du 8 juillet 2019.

²⁷⁷ Délibération n°2/2021 du 4 février 2021.

A. Sur le remplacement de la notion « honorabilité » par la notion de « dangerosité »

L'article 14 paragraphe (1) du projet de loi a été amendé comme suit : « *Les autorisations, permis et agréments prévus par la présente loi sont délivrés par le ministre aux **seules** personnes qui, **compte tenu de leur comportement, de leur état mental et de leurs antécédents judiciaires ou policiers, ne font pas craindre qu'elles sont susceptibles de présenter un danger pour elles-mêmes ou pour autrui, pour l'ordre public ou pour la sécurité publique. Une condamnation pour une infraction intentionnelle violente est considérée comme une indication d'un tel danger.*** »

Les dispositions amendées ont été faites « conformément aux observations du Conseil d'Etat et pour les raisons évoquées par la Haute Corporation ».

Le Conseil d'Etat avait, notamment, estimé dans son avis complémentaire du 19 décembre 2020 que le critère de l'honorabilité est « difficilement transposable à la vérification de l'aptitude d'une personne à détenir ou à manier une arme ».

La Commission nationale s'était ralliée à l'avis du Conseil d'Etat précité « uniquement en ce qu'il n'est pas pertinent d'utiliser la notion d'« honorabilité » pour apprécier si un particulier dispose de l'aptitude requise pour détenir ou manier une arme »²⁷⁸.

Dans la mesure où le terme « honorabilité » a été remplacé par le terme « dangerosité » à l'article 19 (agrément des salariés et collaborateurs des armuriers) et à l'article 24 du projet de loi (octroi des autorisations aux particuliers), elle tient à réitérer les observations suivantes, formulées dans son avis du 4 février 2021, « [n]éanmoins, la référence à la notion d'« honorabilité » pourrait apparaître pertinente en ce qui concerne les agréments qui seraient délivrés par le ministre aux armuriers ou courtiers, lesdits agréments étant un prérequis à l'accès de telles professions. A ce titre, il est précisé qu'en France la notion d'« honorabilité » est utilisée pour toute personne souhaitant « exercer l'activité qui consiste, à titre principal ou accessoire, soit en la fabrication, le commerce, l'échange, la location, la location-vente, le prêt, la modification, la réparation ou la transformation, soit en la négociation ou l'organisation d'opérations en vue de l'achat, de la vente, de la fourniture ou du transfert d'armes, de munitions ou de leurs éléments ». Cependant, cette notion n'est pas reprise pour les personnes souhaitant acquérir ou détenir une arme. En effet, l'article L.312-3-1 du Code de la sécurité intérieure français dispose que « [l]'autorité administrative peut interdire l'acquisition et la détention des armes, munitions et de leurs éléments des catégories A, B et C aux personnes dont le comportement laisse craindre une utilisation dangereuse pour elles-mêmes ou pour autrui ». La Commission nationale reviendra plus en détail sur la référence faite à la notion d'honorabilité dans la législation luxembourgeoise dans son avis sur le projet de loi n°7691, qui vise à harmoniser

²⁷⁸ Délibération n°2/2021 du 4 février 2021, page 8, point I, 1.A, b, ii.

et préciser les différentes procédures de « contrôle d'honorabilité » actuellement prévues dans plusieurs textes de lois. »²⁷⁹.

B. Sur la proposition faite par le Conseil d'Etat dans son avis complémentaire précité selon laquelle il propose le mécanisme d'un avis circonstancié émis par le procureur d'Etat et transmis au ministre

Il ressort du commentaire de l'amendement n°22 que la proposition du Conseil d'Etat d'un « mécanisme d'un avis circonstancié » n'a pas été suivie par les auteurs des amendements.

Ces derniers proposent, en effet, de maintenir l'approche d'une fourniture d'informations au ministre de la Justice « quitte à l'entourer de toutes les conditions requises et nécessaires, plutôt que d'adopter l'approche d'un avis à fournir par le Parquet », sans toutefois préciser ce qu'il convient d'entendre par « conditions requises et nécessaires ».

Ils exposent leurs interrogations et les raisons à l'origine d'une telle position. Ces derniers arguent ainsi que « cette façon de faire ne serait guère de nature à résoudre les problèmes qui se posent. Le Parquet, légitimement, émettrait cet avis sur base des principes qui gouvernent l'opportunité des poursuites, c'est-à-dire des considérations tirées de l'envergure et de la gravité du trouble à l'ordre public, de l'indemnisation de la victime, etc. C'est d'ailleurs ce qu'il avait fait pendant une

certaine période en matière de gardiennage. Cependant, les considérations à tenir en compte en matière d'octroi ou de refus d'autorisations en matière d'armes sont sensiblement différentes et ne poursuivent pas le même objectif. ».

De plus, ils estiment que « cette approche soulève bien d'autres questions : Dans le cas d'un avis positif de la part du Parquet, est-ce que ce dernier serait alors dispensé de toute fourniture d'informations au ministre, de sorte que ce dernier ne pourrait même pas suivre la logique et le raisonnement sur lesquels l'avis positif serait basé ? Et dans le cas d'un avis négatif, quelles seraient les informations que le Parquet devrait alors fournir au ministre ? Il ne faut en effet pas oublier que le demandeur en obtention d'une autorisation d'armes a le droit, en cas de refus de sa demande, de saisir les juridictions administratives en vue de l'annulation du refus. Comment les juridictions administratives pourraient-elles alors apprécier si le refus du ministre est justifié ou non, si le ministre ne peut pas fournir aux juridictions administratives les informations et faits étant à la base de sa décision ? S'y ajoute encore que, rien qu'en prenant en compte le Service Armes & Gardiennage et sans considérer l'ensemble des lois en vigueur au Luxembourg qui requièrent l'évaluation d'une honorabilité ou d'une dangerosité avant l'octroi d'une autorisation administrative, le Parquet serait probablement submergé de demandes d'avis, ce qui l'empêcherait en fait de se consacrer à son activité principale qui est la poursuite des infractions pénales. Le projet de loi

²⁷⁹ Délibération n°2/2021 du 4 février 2021, page 26, l. 6.

n° 7691, qui ne concerne encore que les lois étant de la compétence du ministère de la Justice, permet de se faire une idée du nombre très important d'avis dont le Parquet serait alors saisi, si on optait pour cette approche de l'avis du Parquet en toutes matières. ».

Or, sur ce point, la CNPD s'était interrogée, dans son avis complémentaire du 4 février 2021, si une telle enquête administrative n'aurait pas comme conséquence d'engendrer « une duplication des informations concernant les antécédents judiciaires d'une personne dans les mains de différentes autorités. En effet, la Commission nationale comprend que certaines des données contenues dans les fichiers tenus par la Police grand-ducale, par le Ministère public ou le SRE seront amenées à figurer une nouvelle fois dans un fichier tenu par le ministre »²⁸⁰.

Ainsi, elle tient à réitérer ses considérations suivantes « [a]fin d'éviter une duplication de telles données et la tenue d'une sorte de nouveau « casier bis » par le ministre pour les personnes concernées par la loi en projet, la CNPD estime qu'une méthode moins intrusive pour atteindre le même but devrait être préférée au système actuellement prévu par les auteurs du projet de loi. Elle se rallie, ainsi, à la proposition faite par le Conseil d'Etat dans son avis complémentaire du 19 décembre 2016 selon lequel il propose le mécanisme d'un avis circonstancié émis par le procureur d'État et transmis au ministre. Ce mécanisme se substituerait à la communication au ministre de renseignements par la Police grand-ducale,

le Ministère public et le SRE. Un tel mécanisme permettrait d'éviter une duplication des données concernant les antécédents judiciaires d'un demandeur tout en permettant au ministre d'obtenir les informations nécessaires et pertinentes, sous forme d'un avis, afin de lui permettre d'apprécier l'« honorabilité » d'un demandeur. Un tel mécanisme présente encore l'avantage que l'enquête administrative serait confiée à une autorité répressive, le Ministère public, et non pas à une administration. En effet, une telle autorité serait plus appropriée pour mener une telle enquête eu égard à la nature des données traitées. »²⁸¹.

Par ailleurs, la Commission nationale réitère également ses observations relatives au modèle français et belge qui ont tous deux adopté une approche similaire²⁸².

C. Sur l'insertion d'un alinéa 2 nouveau au paragraphe 3 de l'article 14 du projet de loi

Il ressort du commentaire de l'amendement n°22 qu'« il est proposé d'ajouter encore une restriction aux faits pouvant être communiqués au ministre par l'insertion d'un alinéa 2 nouveau au paragraphe 3, visant à exclure les faits qui, bien que correspondant aux points 1° à 3° de l'alinéa 1er du paragraphe 3, ont fait l'objet d'un acquittement, d'une réhabilitation ou d'une prescription. Cet amendement vise à répondre à une interrogation du Conseil d'Etat. L'hypothèse d'un non-lieu n'a pas été reprise ici, alors que ces faits peuvent faire l'objet d'une reprise de l'information sur charges nouvelles,

²⁸⁰ Délibération n°2/2021 du 4 février 2021, page 8, I, 1, A, b, ii.

²⁸¹ ibidem.

²⁸² Délibération n°2/2021 du 4 février 2021, page 8, I, 1, A, b, iii.

6

ANNEXES

conformément aux articles 135 à 136 du Code de procédure pénale, de sorte que ces faits doivent également pouvoir être pris en compte dans le cadre des procédures administratives concernant les autorisations prévues par le présent projet de loi. »

Il convient de féliciter les auteurs des amendements d'avoir apporté de telles précisions.

Néanmoins, en l'absence des catégories de données qui seraient communiquées au ministre, la CNPD n'est pas en mesure d'apprécier si le principe de minimisation des données serait respecté en l'espèce.

Sur ce point, elle renvoie, de manière générale, à ses développements relatifs au principe de minimisation des données formulés dans son avis complémentaire du 4 février 2021²⁸³.

D. Sur l'échange d'informations entre le Service Armes & Gardiennage et le Service de renseignement de l'Etat

Il y a lieu de relever que le paragraphe (6) de l'article 14 du projet de loi concernant l'échange d'informations entre le Service Armes & Gardiennage et le Service de renseignement de l'Etat demeure inchangé.

Les auteurs des amendements n'apportent pas davantage de précisions à ce sujet dans leur commentaire de l'amendement n°22

mais énoncent les raisons pour lesquelles cet échange d'informations est nécessaire.

Sans préjuger de la nécessité d'un tel échange d'informations, la Commission nationale regrette cependant que ses considérations formulées dans son avis du 4 février 2021 n'aient pas été prises en compte et tient, dès lors, à les réitérer²⁸⁴.

E. Remarques finales

De manière générale, il y a lieu de regretter que l'ensemble des interrogations soulevées dans l'avis complémentaire du 4 février 2021 de la CNPD n'aient pas été prises en considération.

Ainsi, outre les réitérations formulées ci-avant, elle regrette que le texte actuel ne permette pas aux personnes concernées de « *comprendre l'étendue et la portée de l'enquête administrative, ne serait-il pas préférable d'indiquer expressément à l'article 14 nouveau que les données collectées lors de l'enquête administrative proviennent des fichiers tenus par la Police grand-ducale, le Ministère public ou le SRE ?* »²⁸⁵.

De même qu'« à l'instar des dispositions prévues à l'article 26 paragraphes (2) et (3) de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière²⁸⁶, ne faudrait-il pas prévoir dans le projet de loi sous avis que les données transmises au ministre, à des fins d'enquête administrative, ne peuvent être utilisées que

²⁸³ Délibération n°2/2021 du 4 février 2021, page 17, I, 1, F.

²⁸⁴ Délibération n°2/2021 du 4 février 2021, page 17, I, 1, F, b.

²⁸⁵ Délibération n°2/2021 du 4 février 2021, page 10, I, 1, B.

²⁸⁶ L'article 26 paragraphes (2) et (3) dispose que : « (2) Les données et informations transmises ne peuvent être utilisées par l'administration que pour la finalité pour laquelle elles ont été transmises. Elles sont effacées dès que leur conservation n'est plus nécessaire au regard de la finalité pour laquelle elles ont été transmises. (3) La transmission ultérieure des données et informations par l'administration de l'Etat à une tierce personne requiert l'accord préalable écrit de la personne visée à l'article 18, paragraphe 1 er, ayant transmis les données et informations concernées. Le cas échéant, l'article 6, paragraphe 3, est applicable ».

*pour la finalité pour laquelle elles ont été transmises et encadrer la transmission, le cas échéant, par le ministre à une autre administration/ à un tiers ?*²⁸⁷.

En outre, et tel que la CNPD l'avait relevé dans son avis précité, en ce qui concerne le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes, des garanties devraient être prévues « dans le projet de loi alors qu'en l'état actuel du dispositif sous avis, les personnes concernées verront une duplication de leurs données relatives à des condamnations pénales ou à des infractions aux mains de plusieurs autorités. La collecte de telles données lors de l'enquête administrative pourrait aboutir à la tenue d'une sorte de nouveau « casier bis » par le ministre. Celui-ci disposerait, le cas échéant, à l'issue de l'enquête de la copie de rapports de police, extraits de procès-verbaux, jugements, ou encore des « informations nécessaires » fournies par le SRE »²⁸⁸.

Il en va de même en ce qui concerne les traitements de catégories particulières de données pour lesquelles, la CNPD estime, conformément à l'article 9, paragraphe (2), du RGPD, que le projet de loi devrait prévoir des « mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ». Il est renvoyé aux considérations soulevées dans son avis du 4 février 2021²⁸⁹.

Enfin, la Commission nationale regrette encore qu'aucune précision n'ait été apportée, ni en ce qui concerne la durée de conservation des données obtenues dans le cadre de la vérification de l'honorabilité²⁹⁰, ni en ce qui concerne l'autorité de contrôle compétente pour contrôler et surveiller le respect des dispositions légales prévues par l'article 14 du projet de loi²⁹¹. Elle réitère, dès lors, l'ensemble de ses observations à ce sujet.

Pour le surplus, la CNPD renvoie à ses avis des 8 juillet 2019 et 4 février 2021 précités.

Ainsi décidé à Belvaux en date du 1^{er} octobre 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

²⁸⁷ Délibération n°2/2021 du 4 février 2021, page 11, I, 1, C.

²⁸⁸ Délibération n°2/2021 du 4 février 2021, page 12, I, 1, D.

²⁸⁹ Délibération n°2/2021 du 4 février 2021, page 12, I, 1, E.

²⁹⁰ Délibération n°2/2021 du 4 février 2021, page 17, I, 3.

²⁹¹ Délibération n°2/2021 du 4 février 2021, page 17, I, 5.

6

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7818 portant modification du Code de la consommation aux fins de transposition de 1. la directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques ; 2. la directive (UE) 2019/771 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens, modifiant le règlement (UE) 2017/2394 et la directive 2009/22/CE et abrogeant la directive 1999/44/CE. (Délibération n°30/AV25/2021 du 1/10/2021)

Conformément à l'article 57, paragraphe 1^{er}, lettre (c) du règlement (UE) 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 1^{er} 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 13 avril 2021, Madame la Ministre de la Protection des consommateurs

a invité la Commission nationale à se prononcer sur le projet de loi n° 7818 portant modification du Code de la consommation aux fins de transposition de 1. la directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques ; 2. la directive (UE) 2019/771 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens, modifiant le règlement (UE) 2017/2394 et la directive 2009/22/CE et abrogeant la directive 1999/44/CE (ci-après le « projet de loi »).

D'après les auteurs du projet de loi, « [l]e principal objectif de ces directives est de favoriser la création d'un véritable marché numérique dans l'intérêt à la fois des consommateurs et des entreprises en éliminant les principaux obstacles liés au droit des contrats qui entravent le commerce transfrontière ». Les auteurs du projet de loi indiquent que les directives « prévoient des règles d'harmonisation maximale ». Les deux directives à transposer « se basent sur l'article 114 du Traité sur le fonctionnement de l'Union européenne, dont le principal objectif est d'améliorer l'établissement et le fonctionnement du marché intérieur » et s'insèrent dans la « stratégie [de l'Union européenne] pour un marché unique numérique ».

Suivant l'exposé des motifs, le projet de loi « réforme, d'une part, en profondeur les règles relatives à la conformité des biens meubles corporels du Chapitre relatif à la garantie légale

de conformité du Code de la consommation » et « porte, d'autre part, introduction de dispositions nouvelles concernant les contrats de fourniture de contenus numériques ou de services numériques ». Les auteurs du projet de loi expliquent encore que le projet de loi introduit « des dispositions spécifiques pour les biens comportant des éléments numériques (les 'smart goods' tels que les smartphones, les montres connectées, les tablettes numériques, les liseuses etc.) notamment en ce qui concerne leurs mises à jour ». Ensuite, d'après les auteurs du projet de loi, les « dispositions nouvelles concernant les contrats de fourniture de contenus numériques ou de services numériques [...] répondent à la particularité inédite que la fourniture du contenu numérique ou du service numérique peut avoir lieu [...] en l'échange [...] de la fourniture par [le consommateur] de données à caractère personnel ». Finalement, le projet de loi « met subséquentement en place les recours, et leurs modalités, en cas de défaut de fourniture, de non-conformité ou encore de modifications des contenus numériques ou des services numériques ».

Dans la mesure où le présent projet de loi transpose en droit national la directive (UE) 2019/770 et de la directive (UE) 2019/771 précitées, la Commission nationale renvoie en ce qui concerne le cadre légal de cette directive à l'avis 4/2017 du 14 mars 2017 du Contrôleur européen de la protection des données (ci-après le « CEPD ») sur la proposition de directive concernant certains aspects des contrats de fourniture de

contenu numérique²⁹² et limitera ses observations aux dispositions légales concernant la mise en œuvre concrète de cette directive en droit national ayant un impact potentiel en matière de protection des données à caractère personnel.

Mise à jour de « smart goods »

D'après l'exposé des motifs, le projet de loi introduit « des dispositions spécifiques pour les biens comportant des éléments numériques (les 'smart goods' tels que les smartphones, les montres connectées, les tablettes numériques, les liseuses etc.) notamment en ce qui concerne leurs mises à jour ».

Ainsi, le nouvel article L.212-16, paragraphe 2, du Code de la consommation prévoit que

« [l]e professionnel veille à ce que le consommateur soit informé des mises à jour, y compris des mises à jour de sécurité, qui sont nécessaires au maintien de la conformité du contenu numérique ou du service numérique, et les reçoive au cours de la période [...] »

De même, les nouveaux articles L-212-3, alinéa premier, lettre d), L-212-4, paragraphe 3, et L-212-16, paragraphe 2, du Code de la consommation prévoient des obligations et notions similaires concernant les mises à jour et les mises à jour de sécurité.

La CNPD salue l'introduction de telles dispositions qui permettent une utilisation optimale de ces biens comportant des éléments

²⁹² https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_fr.pdf

Voir également : Résumé de l'avis sur la proposition de directive concernant certains aspects des contrats de fourniture de contenu numérique. Journal officiel de l'Union européenne, 2017/C 200/07, 23 juin 2017.

6

ANNEXES

numériques. Ces dispositions clarifient, indépendamment d'autres règles telles que découplant notamment du RGPD, les obligations du professionnel en relation avec la fourniture d'un tel bien.

La Commission nationale tient toutefois à rappeler que de manière complémentaire à cette obligation, lorsque l'utilisation du bien en question implique des traitements de données à caractère personnel, l'article 32 du RGPD prévoit des obligations autonomes en matière de mesures de sécurité, notamment 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 ». À cet égard, il y a lieu de relever que le considérant 30 de la directive 2019/771 précise *in fine* que « [l]a présente directive ne devrait pas avoir d'incidence sur les obligations de fournir des mises à jour de sécurité prévues par ailleurs dans le droit de l'Union ou dans le droit national ».

Le considérant 48 de la directive 2019/770 explique par ailleurs que

« [...] un manquement aux obligations découlant du règlement (UE) 2016/679 pourrait, en même temps, rendre le contenu numérique ou le service numérique impropre à la finalité visée et, en conséquence, constituer un défaut de conformité au critère objectif de conformité qui veut que le contenu numérique ou le service numérique soit adapté aux finalités aux-

quelles servirait normalement un contenu numérique ou un service numérique de même type. [...] »

Dans le même ordre d'idées, le considérant 50 de la directive 2019/770 explique que

« Lorsqu'ils appliquent les règles de la présente directive, les professionnels devraient utiliser des normes, des spécifications techniques ouvertes, des bonnes pratiques et des codes de conduite, y compris en ce qui concerne les formats de données couramment utilisés et lisibles par machine pour extraire le contenu autre que les données à caractère personnel, qui a été fourni ou créé par le consommateur lors de l'utilisation du contenu numérique ou du service numérique, et y compris ceux relatifs à la sécurité des systèmes informatiques et des environnements numériques, qu'ils soient établis au niveau international, au niveau de l'Union ou au niveau sectoriel. »

Ainsi, dans le contexte de la mise à disposition de biens et services impliquant des traitements de données, le défaut de mise en place de mesures de sécurité adéquates (compte tenu de l'état de l'art) par le responsable de traitement ou par le sous-traitant au titre de leurs obligations découlant du RGPD pourrait le cas échéant constituer un défaut de conformité au critère objectif de conformité d'un bien comportant des éléments numériques, et ce même si le contrat avec le consommateur reste muet sur la mise à jour des éléments numériques.

La fourniture de contenus numériques ou de services numériques en échange de la fourniture de données à caractère personnel

Les auteurs du projet de loi précisent dans l'exposé des motifs que

« le projet de loi porte introduction de dispositions nouvelles concernant les contrats de fourniture de contenus numériques ou de services numériques. Ces contrats répondent à la particularité inédite que la fourniture du contenu numérique ou du service numérique peut avoir lieu non seulement en l'échange du paiement d'un prix par le consommateur, mais également de la fourniture par ce dernier de données à caractère personnel ».

Ainsi, le nouvel article L-212-12, paragraphe 1^{er}, alinéa 3 du Code de la consommation prévoit que :

« La présente sous-section s'applique également lorsque le professionnel fournit ou s'engage à fournir un contenu numérique ou un service numérique au consommateur, et le consommateur fournit ou s'engage à fournir des données à caractère personnel au professionnel, sauf lorsque les données à caractère personnel fournies par le consommateur sont exclusivement traitées par le professionnel pour fournir le contenu numérique ou le service numérique conformément à la présente sous-section ou encore pour permettre au professionnel de remplir les obligations légales qui lui incombent, pour autant que

le professionnel ne traite pas ces données à une autre fin. »

Dans le commentaire des articles, les auteurs présentent ce passage comme « [g]rande nouveauté et disposition inédite de la directive 2019/770, les contrats par lesquels au lieu de payer un prix, le consommateur fournit des données à caractère personnel entre dans le champ d'application de la présente sous-section. »

Néanmoins, le nouvel article L.212-12, paragraphe 8 du Code de la consommation indique que :

« Le droit de l'Union européenne en matière de protection des données à caractère personnel s'applique à toutes les données à caractère personnel traitées en lien avec les contrats visés au paragraphe (1).

En particulier, la présente sous-section est sans préjudice du [RGPD] et de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. En cas de conflit entre les dispositions de la présente sous-section et celles du droit de l'Union en matière de protection des données à caractère personnel, ces dernières prévalent. »

En ce qui concerne plus particulièrement la fourniture de contenus numériques ou services numériques, les auteurs du projet de loi précisent dans l'exposé des motifs que

6

ANNEXES

« cette variété de contrats se traduit notamment par une nouveauté notable du texte qui vise à prendre en considération comme contrepartie non pécuniaire de la fourniture du contenu ou du service numérique, la fourniture par le consommateur de données à caractère personnel. La directive tente ainsi de trouver un équilibre entre la protection des données à caractère personnel qui est un droit fondamental et la nécessité de protéger le consommateur dans des transactions s'inscrivant dans un modèle commercial fondé sur la revente de données personnelles ».

En se basant sur les normes européennes en matière de droit fondamental au respect de la vie privée et du droit fondamental à la protection des données à caractère personnel, le CEPD relève qu'il est « fort possible qu'il existe un marché des données à caractère personnel [...] mais cela ne signifie pas que nous puissions ou devons conférer à ce marché l'onction de la loi ». Ainsi, il est regrettable que la directive 2017/770, et partant le projet de loi, suggère que la fourniture de données à caractère personnel puisse constituer une réelle contrepartie à une prestation de services ou de bien, en particulier un contenu ou un service numérique. En effet, tel qu'il découle par ailleurs explicitement du nouvel article L.212-12, paragraphe 8 du Code de la consommation précitée, le traitement des données à caractère personnel du consommateur par le professionnel doit se conformer en tous points aux règles découlant du RGPD et de la législation relative à la vie privée et aux communications électroniques, en particulier

les droits des personnes concernées tels que le droit à l'effacement et le droit d'opposition. À cet égard, la CNPD se rallie à l'avis du CEPD qui considère dans son avis que « les données à caractère personnel ne peuvent pas être comparées à un prix ou à de l'argent » et « que le terme 'les données comme contrepartie' devrait être évité » pour éviter la confusion avec les obligations découlant en particulier du RGPD.

À cet égard, il y a lieu de relever que le considérant 38 de la directive 2019/770 précise que

« la présente directive ne devrait pas réglementer les conditions applicables au traitement licite des données à caractère personnel, cette question étant réglementée, en particulier, par le [RGPD]. Dès lors, un traitement de données à caractère personnel en lien avec un contrat relevant du champ d'application de la présente directive n'est licite que s'il est conforme aux dispositions du [RGPD] concernant les fondements juridiques du traitement des données à caractère personnel ».

En tout état de cause, la CNPD salue néanmoins le fait que le consommateur puisse bénéficier des mêmes garanties prévues par le Code de la consommation en relation avec des contrats soi-disant « gratuits », c'est-à-dire sans contrepartie pécuniaire, portant sur des biens et services numériques, y compris la fourniture de contenu numérique.

Les moyens de recours

D'après l'exposé des motifs, le projet de loi

« met subséquemment en place les recours, et leurs modalités, en cas de défaut de fourniture, de non-conformité ou encore de modifications des contenus numériques ou des services numériques ».

Ainsi, le nouvel article L. 212-6, paragraphe 1^{er}, du Code de la Consommation prévoit que :

« En cas de défaut de conformité, le consommateur a droit, dans les conditions prévues au présent article, à la mise en conformité des biens, à une réduction proportionnelle du prix, ou à la résolution du contrat. »

Le nouvel article L. 212-21, paragraphe 1^{er}, du Code de la Consommation prévoit une disposition similaire pour les contrats visant la fourniture de contenu numérique ou d'un service numérique.

Les auteurs du projet de loi précisent dans le commentaire de cet article que *« lorsque le contenu ou le service numérique a été fourni en échange de la fourniture par le consommateur de données à caractère personnel, le consommateur a droit à la résolution du contrat (il ne peut pas assez logiquement bénéficier d'une réduction du prix) ».*

Comme évoqué plus haut, le considérant 48 de la directive 2019/770 explique que :

« [...] un manquement aux obligations découlant du règlement (UE) 2016/679 pourrait, en même temps, rendre le contenu numérique ou le service numérique impropre à la fina-

lité visée et, en conséquence, constituer un défaut de conformité au critère objectif de conformité qui veut que le contenu numérique ou le service numérique soit adapté aux finalités auxquelles servirait normalement un contenu numérique ou un service numérique de même type.

Tel serait le cas, par exemple, si le professionnel de logiciels de cryptage de données ne mettait pas en œuvre les mesures appropriées requises par le règlement (UE) 2016/679 pour garantir que les données à caractère personnel dès la conception ne sont pas divulguées à des destinataires non autorisés, ce qui rendrait le logiciel de cryptage impropre à sa finalité, à savoir le transfert sécurisé de données par le consommateur à leurs destinataires voulus. Enfin, il pourrait exister des cas où le non-respect, par le professionnel, des obligations qui lui incombent en vertu du règlement (UE) 2016/679 peut également constituer un défaut de conformité du contenu numérique ou du service numérique au critère objectif de conformité qui veut que le contenu numérique ou le service numérique présente les caractéristiques qui sont normales pour des contenus numériques ou des services numériques de même type et auxquelles le consommateur peut raisonnablement s'attendre. Par exemple, si un professionnel proposant une application de vente en ligne ne prend pas les mesures prévues par le règlement (UE) 2016/679 pour assurer le traitement sécurisé des données à caractère personnel du consommateur et

6

ANNEXES

que, par conséquent, les informations liées à la carte de crédit du consommateur sont exposées à des logiciels malveillants ou à des logiciels espions, ce manquement pourrait également constituer un défaut de conformité du contenu numérique ou du service numérique au sens de la présente directive, étant donné que le consommateur pourrait raisonnablement s'attendre à ce qu'une application de ce type possède normalement des caractéristiques empêchant la divulgation de ses coordonnées bancaires.»

Les faits qui mènent à un non-respect des exigences prévues par le règlement (UE) 2016/679, y compris de ses principes de base tels que les exigences en matière de minimisation des données, de protection des données dès la conception et de protection des données par défaut, peuvent également, selon les circonstances, être considérés comme des défauts de conformité du contenu numérique ou du service numérique aux critères subjectifs ou objectifs de conformité prévus par la présente directive. Un exemple pourrait être celui d'un professionnel qui s'engage explicitement dans le contrat à respecter une obligation, ou celui où le contrat peut être interprété comme tel, et où cette obligation est également liée aux obligations du professionnel prévues par le règlement (UE) 2016/679. Dans ce cas, un tel engagement contractuel peut devenir partie intégrante des critères subjectifs de conformité.

[...] Lorsque les faits à l'origine du non-respect des exigences prévues par le règlement (UE) 2016/679 constituent également un défaut de conformité du contenu numérique ou du service numérique aux critères subjectifs ou objectifs de conformité tels qu'ils sont prévus par la présente directive, le consommateur devrait avoir droit aux recours pour défaut de conformité prévus par la présente directive, à moins que le contrat ne soit déjà nul ou susceptible d'être annulé en vertu du droit national.»

Il est ainsi à saluer que, pour des violations du RGPD en lien avec la fourniture d'un contenu numérique, d'un service numérique ou d'un bien comportant des éléments numériques, le consommateur bénéficie des voies de recours susmentionnées, en plus des recours normalement disponibles pour des violations des dispositions en matière de la protection des données à caractère personnel et d'atteintes à la vie privée, notamment à l'article 82 du RGPD. A cet égard, il y a lieu de rappeler le considérant 48 de la directive 2019/770 qui précise que « [l]e règlement (UE) 2016/679 ou toute autre disposition du droit de l'Union en matière de protection des données devrait s'appliquer pleinement au traitement des données à caractère personnel en lien avec tout contrat relevant du champ d'application de la présente directive. En outre, la présente directive devrait s'appliquer sans préjudice des droits, des obligations et des recours non contractuels prévus par le règlement (UE) 2016/679 ».

Toutefois, il n'est pas aisé de déterminer à partir de quels éléments le consommateur pourra effectivement prouver la non-conformité du contrat sur la base d'une violation des dispositions applicables en matière de protection des données. D'une part, la simple allégation d'une telle violation portée à l'encontre d'un professionnel ne semble pas suffisante afin de démontrer une telle non-conformité. D'autre part, l'exigence pour le consommateur d'une décision définitive à l'encontre du responsable du traitement ou d'un sous-traitant de la part de l'autorité de contrôle (en l'occurrence la CNPD) ou dans le cadre d'un recours juridictionnel semble placer une charge de la preuve excessive sur le consommateur, notamment en conditionnant l'exercice de son recours – notamment la résiliation d'un contrat – à des procédures potentiellement longues et éventuellement dépendant d'une marge d'appréciation d'une autorité disposant de l'opportunité d'action. Ainsi, la CNPD se demande s'il ne serait pas utile de détailler de quelle manière le consommateur peut apporter la preuve d'une telle non-conformité.

Au-delà des recours de droit civil disponibles pour le consommateur, il se pose la question de la mise en œuvre de la responsabilité du professionnel, en particulier lorsque la résolution du contrat découle d'un défaut de conformité aux critères subjectifs ou objectifs basés sur une violation des obligations découlant du RGPD. Bien que le droit à un recours collectif ne soit pas visé par les deux directives, la CNPD profite du présent avis pour soutenir l'introduction d'un tel dispositif en droit luxembour-

geois. Ainsi, elle avait déjà appelé de ces vœux l'introduction d'une disposition prévoyant cette possibilité de recours collectif ou « class action » pour des questions de protection des données, dans la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. L'article 80, paragraphe (2) du RGPD indique d'ailleurs explicitement que les États membres peuvent prévoir cette possibilité conformément à leur droit national, ce qui n'est toutefois pas le cas à ce jour au Luxembourg. Une telle possibilité pourrait encore être introduite le cas échéant par le biais du projet de loi n° 7650 portant introduction du recours collectif en droit de la consommation, en y incluant la réparation de préjudices découlant d'une atteinte à la protection des données à caractère personnel ou de la vie privée.

Ainsi décidé à Belvaux en date du 1^{er} octobre 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7762 modifiant la loi du 5 juillet 2016 portant organisation des services de taxis. (Délibération n° 31/AV26/2021 du 1/10/2021)

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 1^{er} 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 27 janvier 2021, Monsieur le Ministre de la Mobilité et des Travaux publics a invité la Commission nationale à se prononcer sur le projet de loi modifiant la loi du 5 juillet 2016 portant organisation des services de taxis (ci-après le « projet de loi »).

Selon l'exposé des motifs, le projet de loi a pour objectif de remédier à certaines défaillances

dans le secteur des taxis ainsi que d'inclure les voitures de location avec chauffeur (ci-après « VLC ») dans la législation.

Le présent avis limitera ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par les articles 11 et 18 du projet de loi sous avis.

1. Sur la condition d'honorabilité

En vertu de l'article 7, paragraphe (2), lettre c) de la loi modifiée du 5 juillet 2016 portant organisation des services de taxis, tel que modifié par le projet de loi, tout conducteur de taxi ou de VLC qui souhaite obtenir une carte de conducteur doit satisfaire aux exigences d'honorabilité spécifiées à l'article 8 de ladite loi.

L'article 11 du projet de loi a pour objet de modifier l'article 8, paragraphes (1) et (2) de la loi du 5 juillet 2016 portant organisation des services de taxis. Il ressort du commentaire de l'article 11 que les auteurs du projet de loi introduisent notamment « *une disposition permettant d'apprécier les antécédents d'une personne encourus pendant les 5 dernières années précédant une demande* ».

A. Sur l'appréciation de l'honorabilité

Il ressort du paragraphe (1) de l'article 8, tel que modifié par l'article 11 du projet de loi, que l'honorabilité s'apprécie « *sur base des antécédents judiciaires qui résultent* » du casier judiciaire du conducteur de taxi ou de VLC.

Le paragraphe (2) de l'article 8 précité, tel que modifié par l'article 11 du projet de loi, énumère quelles seraient les infractions à prendre compte aux fins d'apprécier l'honorabilité d'un conducteur de taxi ou de VLC²⁹³.

S'il y a lieu de relever que la loi précitée ne définit pas la notion d'« honorabilité »²⁹⁴, des précisions quant à l'appréciation de cette notion sont apportées par les travaux parlementaires relatifs à l'article 8 de la loi modifiée du 5 juillet 2016 précitée²⁹⁵, ainsi que par un arrêt de la Cour administrative du Grand-Duché de Luxembourg du 8 novembre 2018²⁹⁶.

Il ressort des travaux parlementaires que l'appréciation de l'honorabilité du conducteur de taxi se base sur le « casier judiciaire N°2 afin de permettre de garantir un standard élevé de sécurité pour les clients »²⁹⁷ et que les « exigences en matière d'honorabilité ont pour intention de tenir compte, lors de la vérification des critères d'attribution, des condamnations éventuelles en relation avec l'activité du conducteur de taxi »²⁹⁸. Il est encore précisé que « [c]ette vérification approfondie est nécessaire en vue de garantir un certain niveau des prestations et d'assurer le sérieux du conducteur qui est responsable du bon transport de ses passagers. De plus, il est ainsi tenu compte du fait que les services de taxi ont un impact considérable sur l'image

*générale du Grand-Duché auprès des visiteurs étrangers »*²⁹⁹.

En outre, la Cour administrative du Grand-Duché de Luxembourg, dans son arrêt du 8 novembre 2018 précité, a été amenée à se prononcer sur l'honorabilité d'un requérant sollicitant une carte de conducteur de taxi conformément à la loi modifiée du 5 juillet 2016 portant organisation des services de taxis³⁰⁰.

Dans cet arrêt, les juges ont estimé que la liste des infractions, visées au paragraphe (2) de l'article 8 de la loi modifiée du 5 juillet 2016 précitée, n'était pas à considérer comme exhaustive et que « *si la personne a fait l'objet d'une condamnation pénale, son honorabilité ne s'en trouve pas automatiquement affectée, mais il appartient au ministre, dans le cadre de l'appréciation de l'honorabilité professionnelle d'un chauffeur de taxi, d'apprécier in concreto si le comportement global de l'intéressé n'est pas tel à le priver de son honorabilité* ».

La Cour a encore retenu que l'appréciation de l'honorabilité ne pouvait pas porter sur des faits commis il y a plus de 5 ans. Ce principe de limitation temporelle, quant aux faits retenus afin d'apprécier l'honorabilité d'un conducteur de taxi, tel que dégagé par la jurisprudence, a été repris par les auteurs du projet de loi à l'article 11 du texte sous avis.

²⁹³ Le paragraphe (2) de l'article 8 de la loi modifiée du 5 juillet 2016 portant organisation des services de taxis, tel que modifié par l'article 11 du projet de loi, dispose que « [l]es exigences en matière d'honorabilité sont satisfaites, en particulier si le conducteur de taxi ou de VLC n'a pas fait l'objet, endéans les cinq ans qui précèdent la demande, d'une condamnation pénale coulée en force de chose jugée prononçant une peine d'emprisonnement d'au moins six mois pour vol, escroquerie, abus de confiance, atteinte volontaire à l'intégrité de la personne, agression sexuelle ou infraction à la législation sur les stupéfiants. ».

²⁹⁴ Quant à l'absence de définition de la notion « d'honorabilité » en droit luxembourgeois, il est renvoyé aux délibérations n°17/2020 du 17 juillet 2020 (points I.2 et I.3.) et n°3/AV3/2021 du 10 février 2021 (point I).

²⁹⁵ Document parlementaire n°6588, commentaire des articles, p.16, ad article 10.

²⁹⁶ Arrêt de la Cour administrative du Grand-Duché de Luxembourg du 8 novembre 2018, numéro 41156C du rôle.

²⁹⁷ Document parlementaire n°6588/00, commentaire des articles, p.16, ad article 10.

²⁹⁸ Document parlementaire n°6588/00, commentaire des articles, p.16, ad article 10.

²⁹⁹ Document parlementaire n°6588/00, commentaire des articles, p.16, ad article 10.

³⁰⁰ Arrêt de la Cour administrative du Grand-Duché de Luxembourg du 8 novembre 2018, numéro 41156C du rôle.

6

ANNEXES

Par conséquent, s'il y a lieu de féliciter les auteurs du projet de loi pour ces précisions, la CNPD regrette que le numéro de bulletin de casier judiciaire qui serait communiqué ne soit pas expressément indiqué dans ledit article alors qu'il ressort des travaux parlementaires précités et de la jurisprudence précitée que le bulletin n°2 serait communiqué. Il y a lieu de rappeler à ce sujet 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.

Dès lors, il conviendrait de compléter le projet de loi en ce sens.

Enfin, sans préjuger de l'appréciation de l'honorabilité *in concreto* devant être faite par le ministre ayant dans ses compétences la loi sous avis (ci-après le « ministre »), et afin de respecter le principe de prévisibilité et de précision auquel doit répondre tout texte légal ou réglementaire³⁰¹, la CNPD se demande s'il ne serait pas opportun, à l'instar des législations belges et françaises, de prévoir une liste exhaustive des infractions qui seraient à prendre en compte lors de l'appréciation de l'honorabilité par le ministre ?

B. Sur le cadre légal national comparé à celui en Belgique et en France

Il est intéressant de noter que la loi tant belge que française prévoient une condition similaire à celle requise par l'article 8 de la loi modifiée du

5 juillet 2016 portant organisation des services de taxis, tel que modifié par l'article 11 du projet de loi.

En effet, en Belgique l'article 9 de l'arrêté du Gouvernement wallon portant exécution du décret du 18 octobre 2007 relatif aux services de taxis et aux services de location de voitures avec chauffeur, tel que modifié, prévoit qu'un chauffeur « *satisfait aux conditions de moralité* » s'il n'a pas fait l'objet d'une condamnation pénale grave coulée en force jugée pour les infractions y listées, à savoir « *1° infraction au Livre II, Titre III, chapitres 1er à V, titre V, chapitres 1er et 2, Titre VII, chapitre V, Titre VIII, chapitres 1er et 2 et Titre VIII du Code pénal ; 2° infraction du troisième et du quatrième degré à la réglementation de la circulation routière ; 3° infraction pour excès de vitesse ; 4° conduite en état d'intoxication alcoolique, d'imprégnation alcoolique, d'ivresse ou sous l'effet d'autres substances qui influencent la capacité de conduite dans le cadre de son activité professionnelle* ».

En France, l'article R.3120-8 du Code des transports français prévoit que « *[n]ul ne peut exercer la profession de conducteur de véhicule de transport public particulier si figure au bulletin n° 2 de son casier judiciaire, ou à son équivalent pour les non-nationaux, l'une des condamnations suivantes :*

1° Une condamnation définitive pour un délit sanctionné en vertu du code de la route par une réduction de la moitié du nombre maximal de points du permis de conduire ;

2° Une condamnation définitive pour conduite

³⁰¹ En ce sens, V. 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; V. entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015.

d'un véhicule sans être titulaire du permis de conduire correspondant à la catégorie du véhicule utilisé ou pour conduite malgré l'annulation du permis de conduire ou malgré l'interdiction d'obtenir la délivrance du permis, ou encore pour refus de restituer son permis de conduire après l'invalidation ou l'annulation de celui-ci;
3° Une condamnation définitive prononcée par une juridiction, française ou étrangère, à une peine criminelle ou à une peine correctionnelle d'au moins six mois d'emprisonnement pour vol, escroquerie, abus de confiance, atteinte volontaire à l'intégrité de la personne, agression sexuelle, trafic d'armes, extorsion de fonds ou infraction à la législation sur les stupéfiants. »

Contrairement au cadre légal national actuel, les lois belge et française énumèrent limitativement les faits sur lesquels portera l'appréciation de la « moralité » ou de « l'honorabilité professionnelle »³⁰² d'un conducteur. Dès lors, afin de répondre aux exigences de précision et de prévisibilité auxquelles doit répondre un texte légal³⁰³, la CNPD se demande si les auteurs du projet de loi ne devraient pas s'inspirer des dispositions légales belges et françaises précitées ?

2. Sur la banque de données dédiée à la gestion journalière des licences d'exploitation de taxis et de VLC ainsi qu'à celles des cartes de conducteurs

Il y a lieu de relever que le principe de la création d'une banque de données à caractère personnel tenue par le ministre et dédiée à la gestion journalière des licences d'exploitation de taxi a

été introduit par l'article 18 de la loi modifiée du 5 juillet 2016 portant organisation des services de taxis.

L'article 23 du projet de loi entend cependant procéder à une refonte complète de ces dispositions. La Commission nationale regrette que les raisons ayant poussé les auteurs du projet de loi à procéder à une telle refonte ne soient pas exposées dans le commentaire des articles, alors que les nouvelles dispositions manquent de clarté et de précisions, contrairement à celles qui figuraient initialement à l'article 18 précité.

A. Remarques préliminaires

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.

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'Etat 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

³⁰² Article R.3120-6, point 3° du Code des transports français.

³⁰³ En ce sens, V. 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; V. entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015.

6

ANNEXES

ou au droit d'un Etat 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.

Ainsi, bien que les dispositions de l'article 18 précité prévoyaient d'ores et déjà la tenue d'un fichier par le ministre, celles-ci devraient, à la suite de leur refonte par l'article 23 du projet de loi, être complétées alors qu'elles sont formulées de manière trop vague ou imprécise.

Dans les développements ci-après, la Commission nationale reviendra sur les dispositions devant être complétées ou sur les éléments devant être précisés.

B. Sur le rôle des différents acteurs

La Commission nationale se félicite que le paragraphe (4) de l'article 18 de la loi modifiée du 5 juillet 2016 portant organisation des services de taxis, tel que modifié par l'article 23 du projet de loi, précise le rôle des différents acteurs dans le cadre des traitements de données à caractère personnel visés par l'article précité.

La CNPD salue que les auteurs du projet de loi aient précisé que :

- le ministre a la qualité de responsable du traitement au sens de l'article 4, point 7) du RGPD ; et que
- le CTIE et la Société Nationale de Circulation Automobile (ci-après la « SNCA ») agissent en tant que sous-traitant du ministre au sens de l'article 4, point 8) du RGPD.

Concernant le rôle du sous-traitant, il y a lieu de rappeler que conformément à l'article 28 du RGPD, celui-ci « *ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement* ».

C. Sur les finalités du traitement de données à caractère personnel

Comme relevé précédemment, l'article 23 procède à une refonte de l'article 18 de la loi modifiée du 5 juillet 2016 portant organisation des services de taxis. Il résulte de cette refonte que les finalités énumérées au paragraphe (1) de l'article 18 précité sont supprimées par l'article 23 du projet de loi. Les finalités du traitement sont désormais

énumérées au paragraphe (2) de l'article 18, tel que modifié par l'article 23 du projet de loi.

Si ledit article reprend sensiblement les finalités qui étaient listées à l'article 18, paragraphe (1), il y a lieu de relever que la finalité relative à « *la mise en œuvre d'analyses et de recherches à des fins de planification et d'évaluation de la qualité des services de taxi après dépersonnalisation des données afférentes* » a été supprimée. L'article 23 du projet de loi introduit également une nouvelle finalité à savoir « *le contrôle du respect des dispositions de la présente loi et de ses règlements d'exécution* ».

La Commission nationale se félicite que les finalités soient déterminées et listées au paragraphe (2) de l'article 18, tel que modifié par l'article 23 du projet de loi.

Néanmoins, pour plus de clarté il aurait été préférable que les auteurs du projet de loi précisent quelles données sont collectées et pour quelles finalités. En l'absence de telles précisions, il est difficile pour la CNPD d'apprécier si le principe de minimisation serait respecté. Il est rappelé qu'en vertu de ce principe, seules les données à caractère personnel qui sont nécessaires à la réalisation des finalités peuvent être traitées.

D. Sur l'origine des données à caractère personnel et les catégories de données à caractère personnel

La Commission nationale se félicite que les catégories de données à caractère personnel collectées par le ministre soient énumérées au

paragraphe (3) de l'article 18, tel que modifié par l'article 23 du projet de loi. Cependant, il y a lieu de relever que la formulation initiale de l'article 18 était plus précise tant en ce qui concerne les catégories de données à caractère personnel collectées par le ministre que leurs origines. Or, de telles dispositions ont été supprimées et n'ont pas été reprises par l'article 23 du projet de loi.

i. Sur l'origine des données

Il convient de noter que l'article 18, dans sa version initiale, opérait une distinction entre les catégories de données qui étaient collectées directement auprès des personnes concernées de celles qui étaient collectées indirectement et qui provenaient de fichiers étatiques.

La formulation actuelle n'opère plus une telle distinction. Toutefois, il ressort du commentaire des articles que « *[l]'accès à la majorité des données personnelles se fait moyennant l'accès à d'autres bases de données existantes telles que le RNPP ou la base de données sur les véhicules* » et que « *les encodages de nouvelles données personnelles sont très limités au sein de la base de données* ». En outre, le paragraphe (5) de l'article 18, tel que modifié par l'article 23 du projet de loi, prévoit également une collecte indirecte de données par le ministre via la SNCA.

Dès lors, la CNPD s'interroge sur le bienfondé de la suppression des dispositions de l'article 18, dans sa version initiale, qui spécifiait l'origine des données collectées et traitées par le ministre.

6

ANNEXES

Si un accès à des fichiers étatiques devaient être un moyen de collecter les données à caractère personnel alors cela devrait figurer expressément dans le projet de loi. La Commission nationale y reviendra *infra* au point E.

Enfin, il y a lieu de noter qu'en vertu du paragraphe (5) de l'article 18, tel que modifié par l'article 23 du projet de loi, le ministre obtiendrait via la SNCA « *le numéro d'identification national du candidat* ». Or, il convient de rappeler que l'accès au RNPP par une administration devrait 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. Il serait, dès lors, préférable de prévoir que le ministre ait accès au RNPP conformément aux dispositions précitées plutôt que de prévoir la transmission du numéro d'identification national par la SNCA au ministre.

ii. Sur les catégories de données à caractère personnel

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. Le RGPD ne s'appliquera donc qu'aux données à caractère personnel qui seraient communiquées au ministre.

Il convient de relever que la version initiale de l'article 18 était rédigé avec plus de précision et de clarté en ce qui concerne les catégories de données collectées par le ministre. En effet, le paragraphe (3) de l'article 18 énumérait les catégories de données collectées indirectement via des fichiers étatiques et le paragraphe (5) énumérait quant à lui les catégories de données qui étaient collectées directement auprès des conducteurs, exploitants de taxis ou intéressés « *figurant sur la liste d'attente* ».

Or, la formulation actuelle de l'article 18, tel que modifié par l'article 23 du projet de loi, propose une énumération succincte et imprécise, qui ne reprend pas certaines des catégories de données qui étaient pourtant visées par les dispositions supprimées. De plus, les dispositions sous avis ne mentionnent pas à quelle personne concernée se rapportent les données à caractère personnel qui seraient collectées.

A titre d'illustration, il convient de relever que le paragraphe (3) de l'article 18, tel que modifié par l'article 23 du projet de loi, prévoit que

« *les noms et prénoms* » seraient collectées. S'agit-il des noms et prénoms des conducteurs, exploitants de taxi ou de VLC ?

Ainsi, afin de répondre aux exigences de précision et de prévisibilité auxquelles doit répondre un texte légal³⁰⁴, la Commission nationale suggère que les auteurs du projet reprennent la formulation initiale de l'article 18, paragraphes (3) et (5), sinon de préciser dans le texte sous avis à quelle personne concernée se rapportent les catégories de données à caractère personnel et compléter l'énumération des catégories de données à caractère personnel, qui n'apparaît pas à ce stade complète. Il conviendrait, par exemple, de préciser que la photo du conducteur serait collectée ainsi que l'extrait de casier judiciaire d'un conducteur de taxi ou de VLC serait collecté.

Enfin, une erreur matérielle semble s'être glissée au paragraphe (3) de l'article 18, tel que modifié par l'article 23, en ce qu'il dispose « *pour les fichiers énumérés aux paragraphes 1^{er} et 2* » alors qu'il ressort desdits paragraphes que le ministre tient une seule banque de données. De plus, au même paragraphe, il semble également que les auteurs du projet de loi aient omis le terme « *collectées* » juste après « *les données à caractère personnel* ».

E. Sur l'accès au RNPP et à la base de données sur les véhicules

Il convient de relever que les dispositions initiales de l'article 18, paragraphe (3), encadraient

l'accès à d'autres fichiers étatiques par le ministre. En effet, cet article précisait pour chacun des fichiers auxquels le ministre pouvait accéder quelles étaient les données qu'il pouvait collecter pour les finalités y énumérées.

Or, ces dispositions ont été supprimées par l'article 23 du projet de loi bien que les auteurs du projet de loi précisent dans le commentaire des articles que « *[l']accès à la majorité des données personnelles se fait moyennant l'accès à d'autres bases de données existantes telles que le RNPP ou la base de données sur les véhicules* ».

Si l'accès à d'autres bases de données étatiques semble être toujours la volonté des auteurs du projet de loi, cela n'est désormais plus reflété dans la formulation actuelle de l'article 18, tel que modifié par l'article 23 du projet de loi. L'article 18 paragraphe (5), tel que modifié par l'article 23 du projet de loi, ne prévoyant en outre qu'une communication de données de la SNCA vers le ministre.

Dès lors, afin de répondre aux exigences de précision et de prévisibilité auxquelles doit répondre un texte légal³⁰⁵, la Commission nationale estime que de tels accès devraient être prévus et encadrés par le projet de loi. Sur ce point, il est suggéré aux auteurs du projet de loi de reprendre les dispositions de l'article 18, paragraphe (3).

Enfin, il y a lieu d'attirer l'attention des auteurs du projet de loi sur le fait que ces accès ne doivent

³⁰⁴ En ce sens, V. 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; V. entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015.

³⁰⁵ En ce sens, V. 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; V. entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015.

6

ANNEXES

pas permettre au ministre d'obtenir de manière indirecte des données à caractère personnel issues de fichiers d'autorités étatiques pour lesquels il n'aurait pas accès en vertu du projet de loi sous avis.

F. Sur la communication des données à caractère personnel à la SNCA

Il y a lieu de relever que dans sa version initiale l'article 18, paragraphe (10) disposait que « *[l]e ministre est autorisé à communiquer, par des procédés informatisés, ou non, des données à caractère personnel relatives aux exploitants ou conducteurs, à la SNCA, aux fins de permettre la vérification d'une licence d'exploitation en cours de traitement et aux fins de délivrance et d'apposition du tableau taxi, de la plaque zone taxi et du panneau lumineux. Les données qui peuvent être communiquées à la SNCA sont déterminées par règlement grand-ducal.* »

L'article 14, paragraphe (2), du règlement grand-ducal du 23 juillet 2016 fixant notamment les modalités d'application de la législation portant organisation des services de taxis, énumère les données qui peuvent être communiquées par le ministre à la SNCA.

Dans la mesure où les dispositions du paragraphe (10) de l'article 18 sont supprimées par l'article 23 du projet de loi, et que les auteurs du projet de loi n'indiquent pas les raisons d'une telle suppression, la Commission nationale se demande si une telle communication reste prévue ? Dans l'affirmative, de telles précisions

devraient être apportées par les auteurs du projet de loi.

G. Sur l'accès aux données à caractère personnel

Il convient de relever que les dispositions énoncées au paragraphe (7) de l'article 18, tel que modifié par l'article 23 du projet de loi, prévoient un accès « *aux données contenues dans la banque de données* » pour les membres de la Police grand-ducale et les agents de l'administration des douanes et accises dans le cadre de la finalité visée par le paragraphe (2), point 1) de l'article précité.

Or, dans la mesure où 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 elles³⁰⁶, il conviendrait de préciser le cadre légal des contrôles pouvant être effectués par les membres de la Police grand-ducale et les agents de l'administration des douanes et accises. La Commission nationale recommande, dès lors, d'insérer à la fin du paragraphe (7) de l'article 18, tel que modifié par l'article 23 du projet de loi, la formulation suivante : « *conformément à leurs pouvoirs de contrôle tels que visés à l'article 22 de la présente loi* »³⁰⁷.

Enfin, la CNPD se demande encore si l'accès à un tel fichier par la Police grand-ducale ne devrait pas être prévu dans le corps de l'article 43 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, qui précise notamment

³⁰⁶ Voir entre autres CourEDH, Zakharov c. Russie [GC], n°47413/06, § 228-229, 4 décembre 2015.

³⁰⁷ L'article 22 de la loi modifiée du 5 juillet 2016 portant organisation des services de taxis dispose que : « *[l]es infractions aux dispositions de la présente loi et à ses règlements d'exécution sont recherchées et constatées par les membres de la Police grand-ducale et par les fonctionnaires de l'Administration des douanes et accises.* »

les fichiers auxquels les forces de l'ordre peuvent avoir accès, ainsi que les conditions dans lesquelles de tels accès peuvent être opérés. Ce d'autant plus alors que le projet de loi n°7741 portant modification 1° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, 2° de la loi modifiée du 5 juillet 2016 portant réorganisation du SRE et 3° du Code pénal, entend modifier ledit article. En effet, il ressort de l'exposé des motifs du projet de loi N°7741 précité, que la modification envisagée de l'article 43 précité « a pour but d'adapter la liste des fichiers déjà accessibles à la Police et de mieux encadrer leur accès par la Police ».

H. Sur la traçabilité des accès

Il y a lieu de relever que le paragraphe (6) de l'article 18 prévoyait des dispositions spécifiques quant à la traçabilité des accès, qui se voient désormais être supprimées par l'article 23 du projet de loi. Si le RGPD ne prévoit pas explicitement que de telles dispositions soient reflétées dans un texte de loi, la Commission nationale tient toutefois à rappeler le principe d'intégrité et confidentialité qui doit être respecté par le responsable du traitement, en l'occurrence le ministre.

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) ».

En outre, 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.

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. Dans ce contexte, il est vivement recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début la personne ou le service, au sein de chaque entité ou administration concernée, qui aurait accès aux données ou, dans le cadre des administrations, à l'interface informatique mise à disposition par le CTIE, et à quelles données précises cette personne ou ce service aurait accès.

En outre, il est nécessaire de prévoir un système de journalisation des accès (registre des logs), afin de pouvoir garantir la traçabilité des accès. Enfin, la CNPD recommande que les données de journalisation soient conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.

6

ANNEXES

La CNPD souligne aussi l'importance d'effectuer pro activement des contrôles en interne. A cet effet, il convient conformément à l'article 32, paragraphe (1), lettre d) du RGPD de mettre en œuvre une procédure « *visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».

I. Sur la durée de conservation des données à caractère personnel

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.

La Commission nationale se félicite que l'article 18, paragraphe (8), tel que modifié par l'article 23 du projet de loi dispose que « *[l]es données seront conservées au maximum trois ans après la déchéance de la licence d'exploitation de taxi, de la licence d'exploitation de VLC ou de la carte de conducteur. La photo d'identité est détruite après la production de la carte de conducteur* ».

Cependant, de telles dispositions respectent-elles le principe de limitation de la conservation en ce qui concerne l'extrait de casier judiciaire qui serait collecté en vertu de l'article 8 de la loi du 5 juillet 2016 portant organisation des services de taxis ?

Enfin, il y a encore lieu de relever que le texte en projet prévoit une durée de conservation qu'en cas de déchéance d'une licence d'exploitation de taxi, de VLC ou d'une carte de conducteur. Cependant, qu'en est-il en cas de renouvellement d'une licence d'exploitation de taxi, de VLC ou d'une carte de conducteur ?

Il est rappelé à ce titre que conformément au principe d'exactitude, les données personnelles doivent être exactes, et si nécessaire, tenues à jour. Ainsi, il incombe au responsable du traitement de prendre toutes les mesures raisonnables afin de garantir que les données personnelles inexactes soient rectifiées ou supprimées sans tarder.

Ainsi décidé à Belvaux en date du 1er octobre 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 ailleurs, conformément à l'article 8 point 3^o de ladite loi du 1^{er} août 2018 (transposant en droit national l'article 46, paragraphe 1^{er}, lettre (c) de la directive (UE) n° 2016/680), 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 8 février 2021, Madame la Ministre de la Justice a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal portant organisation des régimes internes des centres pénitentiaires (ci-après le « projet de règlement grand-ducal »).

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal portant organisation des régimes internes des centres pénitentiaires.

(Délibération n°32/AV27/2021 du 1/10/2021)

Par courrier en date du 16 juin 2021, Madame la Ministre de la Justice a invité la Commission nationale à se prononcer sur l'amendement gouvernemental relatif au même projet.

Selon l'exposé des motifs, le projet de règlement grand-ducal a pour objet de « fixer les règles relatives au régime pénitentiaire des centres pénitentiaires luxembourgeois » et abrogera le règlement grand-ducal modifié du 24 mars 1989 concernant l'administration et le régime interne des établissements pénitentiaires.

Les auteurs du projet de règlement grand-ducal précisent encore que figure dans le projet de règlement grand-ducal « un chapitre dédié au traitement des données à caractère personnel des détenus. Suite à l'entrée en vigueur de la législation en matière de protection des données personnelles des règles strictes concernant le traitement des données sont applicables. Il revient au responsable du traitement des données d'en fixer les règles et les conditions générales ».

La Commission nationale limitera ses observations aux questions ayant trait à la protection des données à caractère personnel, soulevées par le Chapitre VIII et les articles 103 et 121 du projet de règlement grand-ducal.

6

ANNEXES

I. Sur les traitements de données effectuées par l'administration pénitentiaire

L'article 127, paragraphe (1), du projet de règlement grand-ducal a pour objet d'énumérer les catégories de données qui seraient traitées par l'administration pénitentiaire dans le cadre de ses missions visées à l'article 3 de la loi du 20 juillet 2018 portant réforme de l'administration pénitentiaire.

1. Remarques liminaires

Il ressort du commentaire des articles que les données énumérées au paragraphe (1) de l'article 127 du projet de loi « *étaient déjà traitées sur base de l'article 43 du règlement du 24 mars 1989. Eu égard aux dispositions de la loi du 1^{er} 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 a été considéré comme utile tout d'abord d'effectuer un tri dans les registres énumérés à l'article 43 du règlement précité de 1989, alors que certains registres n'existent plus à l'heure actuelle, et par ailleurs, d'énumérer de manière détaillée toutes les données qui seront dorénavant traitées par l'administration pénitentiaire* ».

L'article 43 du règlement grand-ducal du 24 mars 1989 concernant l'administration et le régime interne des établissements pénitentiaires, qui sera abrogé par le projet de règlement grand-ducal, listait 16 registres à savoir :

1. le registre des peines ;
2. le registre des personnes mises à la disposition du Gouvernement pour vagabondage et mendicité ou en vertu d'une mesure prise en exécution de l'article 15 de la loi du 28 mars 1972 concernant l'entrée et le séjour des étrangers ;
3. le registre des prévenus qui se trouvent sous mandat d'amener, mandat de dépôt ou mandat d'arrêt ;
4. le registre des mineurs placés à la section disciplinaire ;
5. le registre des détenus militaires ;
6. le registre de l'état journalier de la population pénitentiaire ;
7. le registre des punitions ;
8. le registre des valeurs en numéraire déposées par les détenus et
9. le répertoire alphabétique des détenus ;
10. le répertoire alphabétique de la correspondance des détenus ;
11. les dossiers individuels des détenus ;
12. le registre des déclarations d'opposition ;
13. le registre des déclarations d'appel et des pourvois en cassation ;
14. l'agenda des élargissements ;
15. le registre faisant mention des reclus volontaires d'après l'article 332 du règlement ; et
16. le registre des élections de domicile.

Désormais, le projet de règlement grand-ducal ne semble en prévoir que 6, à savoir :

- le registre d'admission³⁰⁸ ;
- le dossier individuel³⁰⁹ ;
- le dossier d'insertion sociale³¹⁰ ;
- le registre des fouilles³¹¹ ;

³⁰⁸ Voir article 128 du projet de règlement grand-ducal.

³⁰⁹ Voir article 129 du projet de règlement grand-ducal.

³¹⁰ Voir article 130 du projet de règlement grand-ducal.

³¹¹ Voir article 121 du projet de règlement grand-ducal.

- le registre visé à l'article 123 du projet de règlement grand-ducal ; et
- le registre des visites³¹².

Par ailleurs, la CNPD comprend que certaines des catégories de données listées à l'article 127, paragraphe (1), du projet de règlement grand-ducal ont vocation à se retrouver dans les registres susmentionnés.

2. Sur le responsable du traitement

Selon les dispositions de l'article 127, paragraphe (1), du projet de règlement grand-ducal, l'administration pénitentiaire traitera les données y énumérées. La Commission nationale comprend dès lors que l'administration pénitentiaire serait à qualifier de responsable du traitement.

Selon l'article 4 de la loi du 20 juillet 2018 portant réforme de l'administration pénitentiaire, l'administration pénitentiaire comprend la direction, le centre pénitentiaire d'Uerschterhaff, le centre pénitentiaire de Luxembourg, le centre pénitentiaire de Givenich et l'institut de formation pénitentiaire.

Dans la mesure où l'administration pénitentiaire englobe plusieurs organes, la Commission nationale se demande si les organes la constituant ne seraient pas, pour certains traitements de données, à qualifier de responsables de traitement séparés.

En effet, et à titre d'exemple, les articles 128 et 129 du projet de règlement grand-ducal se

réfèrent à des registres qui seraient tenus par le greffe des centres pénitentiaires. La tenue de tels registres par les centres pénitentiaires suggère que ces derniers seraient à qualifier de responsables de traitement.

Des clarifications à ce sujet mériteraient d'être apportées par les auteurs du projet de règlement grand-ducal.

3. Sur les finalités des traitements de données à caractère personnel

Comme relevé précédemment, l'article 127 du projet de règlement grand-ducal, a pour objet d'énumérer à son paragraphe (1), les catégories de données qui seraient traitées par l'administration pénitentiaire conformément à l'article 3, paragraphe (4), de la loi du 20 juillet 2018 portant réforme de l'administration pénitentiaire.

L'article 3, paragraphe (4), de la loi du 20 juillet 2018 portant réforme de l'administration pénitentiaire dispose que « *[l]administration pénitentiaire est autorisée à traiter les données à caractère personnel relatives aux personnes dont elle a la charge et celles relatives aux infractions, aux condamnations et autres décisions judiciaires. Ces données ne peuvent être traitées qu'en vue des finalités visées aux articles 1^{er}, paragraphe 2, et 37* ».

L'article 1, paragraphe (2), de la loi précitée dispose notamment que « *[l]objectif de la mise en œuvre des peines privatives de liberté est de concilier la protection de la*

³¹² Voir article 103 du projet de règlement grand-ducal.

6

ANNEXES

société, la sanction du condamné et les intérêts de la victime avec la nécessité de préparer l'insertion de la personne détenue afin de lui permettre de mener une vie responsable et de prévenir la commission de nouvelles infractions.».

L'article 37, paragraphe (1), de la loi précitée dispose encore que « [l]'accès de toute personne, y compris de celles visées à l'article 24, à un centre pénitentiaire peut être soumis à un contrôle de sécurité et de sûreté de la personne, de son identité, de ses bagages et effets personnels, ainsi que du véhicule et de son chargement lorsque ce véhicule entre dans l'enceinte du centre pénitentiaire. Ce contrôle ne peut pas porter sur des dossiers, documents ou pièces qui sont couverts par un secret professionnel ou qui relèvent du secret de l'instruction. Les porte-documents ou autres récipients dans lesquels se trouvent les dossiers, documents ou pièces concernés ne peuvent faire l'objet que d'un contrôle visuel sommaire permettant de constater qu'ils ne contiennent pas d'objets, matières et substances prohibés par la loi ou interdits par règlement grand-ducal pris sur base de l'article 36, paragraphe 2, à l'exclusion de tout contrôle qui permettrait de prendre connaissance du contenu des dossiers, documents ou pièces concernés ».

Par ailleurs, il y a lieu de relever qu'il résulte des travaux préparatoires de la loi du 1^{er} août 2018 relative à la protection des personnes physiques à l'égard des traitements en matière pénale ainsi qu'en matière de sécurité nationale

que « [l]'administration pénitentiaire, pour sa part, sera soumise tantôt aux dispositions du règlement (UE) n° 2016/679, tantôt à celles de la future loi transposant la directive (UE) n° 2016/680, en fonction de la finalité exacte du traitement de données à caractère personnel : s'il s'agit de données que l'administration pénitentiaire traite pour mettre en œuvre les décisions prises dans le cadre de l'exécution des peines, les dispositions de la future loi seront d'application; en revanche, s'il s'agit de traitements de données à caractère personnel ayant comme finalité la simple gestion des centres pénitentiaires, comme par exemple la gestion des badges d'entrée ou des visiteurs, le règlement (UE) n° 2016/679 sera d'application. ».

Dès lors, afin de déterminer les dispositions qui seraient applicables aux traitements de données effectuées par l'administration pénitentiaire dans le cadre du projet de règlement grand-ducal, une attention particulière devrait être portée aux finalités qui seraient poursuivies par le responsable du traitement.

Or, il y a lieu de regretter que les auteurs du projet de règlement grand-ducal ne se réfèrent qu'à la loi du 1^{er} août 2018 relative à la protection des personnes physiques à l'égard des traitements en matière pénale ainsi qu'en matière de sécurité nationale.

En effet, la CNPD estime que les traitements effectués dans le cadre de l'article 37, paragraphe (1), de la loi du 20 juillet 2018

portant réforme de l'administration pénitentiaire devraient être soumis aux dispositions du RGPD.

4. Sur les catégories de données collectées par « l'administration pénitentiaire »

La CNPD se félicite que l'article 127, paragraphe (1) du projet de règlement grand-ducal énumère les catégories de données amenées à être traitées par le responsable du traitement.

Toutefois, certaines imprécisions demeurent, de sorte que la Commission nationale entend formuler les observations ci-après.

A. Sur les données relatives aux mineurs

La CNPD comprend que des données à caractère personnel relatives à des mineurs seraient susceptibles d'être traitées.

En effet, il résulte de l'article 6 de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse, qu'un mineur peut être placé dans un établissement disciplinaire de l'Etat, soit au Centre pénitentiaire de Luxembourg, si une mesure de placement dans un établissement ordinaire de garde, d'éducation ou de préservation est inadéquate en raison de la mauvaise conduite ou du comportement dangereux du mineur en cause.

Or, il y a lieu d'attirer l'attention des auteurs du projet de règlement grand-ducal sur le consi-

dérant 50 de la directive 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 qui énonce que « *les mesures prises par le responsable du traitement devraient comprendre l'établissement et la mise en œuvre de garanties spécifiques destinées au traitement de données à caractère personnel relatives aux personnes physiques vulnérables telles que les enfants* ».

B. Sur les catégories particulières de données

L'article 127, paragraphe (1), du projet de règlement grand-ducal dispose notamment que « *l'administration pénitentiaire peut traiter (...)* 2° *toute documentation constatant des blessures visibles subies antérieurement à son admission au centre pénitentiaire ; (...)* 11° *les noms et prénoms des personnes à prévenir en cas de (...) maladie grave ou de décès ;* 12° *les informations contenues dans les bilans de suivi psychologique, psychosocial et psychothérapeutique des détenus ;* 13° *les informations contenues dans les rapports d'expertise* ».

La CNPD comprend que les rapports d'expertise susvisés font référence aux rapports d'expertise visés à l'article 17, paragraphe (1), de la loi du 20 juillet 2018 portant réforme de l'administration pénitentiaire qui dispose que « *[l']administration pénitentiaire reçoit de plein droit, au moment de la mise en détention d'une personne, copie de la décision judiciaire sur base de laquelle la*

6

ANNEXES

détention est effectuée, ainsi que des rapports d'expertise qui concernent le détenu ».

Les auteurs du projet de loi N°7042 portant réforme de l'administration pénitentiaire avaient précisé au sujet de ces rapports que « [s]ont visés par cela principalement les rapports relatifs à la santé physique et psychique du concerné »³¹³.

Les informations contenues dans de tels rapports sont, dès lors, susceptibles d'être relatifs à la santé physique et psychique du détenu concerné.

Ainsi, les informations précitées visées à l'article 127, paragraphe (1), du projet de règlement grand-ducal sont susceptibles d'être qualifiées de catégories particulières de données dans la mesure où celles-ci sont susceptibles de se rapporter à l'état de santé du détenu.

Par ailleurs, si de tels traitements sont effectués dans le cadre de la mise en œuvre de décisions prises dans le cadre de l'exécution des peines alors les dispositions de l'article 9 de la loi du 1^{er} 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 seront applicables. *A contrario*, si les traitements sont effectués à des fins de gestion des centres pénitentiaires alors les dispositions de l'article 9 du RGPD seront applicables.

a. Sur le respect des dispositions légales spécifiques relatives aux catégories particulières de données

Il y a lieu de relever que les traitements de catégories particulières de données requièrent une protection spécifique et sont soumis à des exigences plus strictes.

Ainsi, si la loi du 1^{er} 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 a vocation à s'appliquer, alors les dispositions prévues à son article 9 seront applicables.

Ces dispositions prévoient notamment que de tels traitements sont autorisés « *uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et uniquement :*

- a) *lorsqu'ils sont autorisés par le droit de l'Union européenne ou en application de la présente loi ou d'une autre disposition du droit luxembourgeois ;*
- b) *pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique, ou*
- c) *lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée ».*

Le chapitre VIII du projet de règlement grand-ducal ainsi que les commentaires des articles

³¹³ Voir projet de loi, document parlementaire n°7042/00, Ad article 18, page 33.

ne précisent cependant pas quelles seraient les garanties appropriées qui seraient mises en œuvre par le responsable du traitement.

La CNPD estime qu'il est important, compte tenu de la nature des données en cause, que de telles garanties soient prévues par le responsable du traitement.

En outre, si le RGPD a vocation à s'appliquer alors les dispositions de l'article 9 du RGPD s'appliqueront.

Cet article prévoit qu'en principe de tels traitements de données sont interdits sauf si l'une des conditions visées au paragraphe (2) de l'article précité est remplie.

Dans le cas présent, la Commission nationale estime que de tels traitements de données pourraient reposer sur l'article 9, paragraphe (2), lettre h), du RGPD qui dispose que « *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* ».

Ainsi, les auteurs du projet de règlement grand-ducal devraient particulièrement être attentifs

aux « *mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée* » qui devraient être mises en œuvre par le responsable du traitement dans le cadre des traitements de catégories particulières de données.

b. Sur l'origine des catégories particulières des données

i. Sur « les informations contenues dans les bilans de suivi psychologique, psychosocial et psychothérapeutiques »

Bien que le projet de règlement grand-ducal précise que les « *informations contenues dans les bilans de suivi psychologique, psychosocial et psychothérapeutiques* » figurent dans le dossier individuel³¹⁴ et dans le dossier d'insertion sociale du détenu³¹⁵, il y a lieu de s'interroger sur l'origine des « *informations contenues dans les bilans de suivi psychologique, psychosocial et psychothérapeutiques* ».

La CNPD se demande si les « *informations contenues dans les bilans de suivi psychologique, psychosocial et psychothérapeutiques* » proviendraient du dossier médical du détenu.

Si tel devait être le cas, il y a lieu de relever que l'article 26, paragraphe (4), de la loi du 20 juillet 2018 portant réforme de l'administration pénitentiaire dispose que « *[l]es prestations de soins de santé sont documentées par le*

³¹⁴ Article 129 du projet de règlement grand-ducal.

³¹⁵ Article 130 du projet de règlement grand-ducal.

6

ANNEXES

médecin traitant du détenu dans un dossier médical. Sans préjudice du secret professionnel visé à l'article 458 du Code pénal ou de toute autre obligation de confidentialité professionnelle, le médecin traitant du détenu ainsi que tous les autres professionnels le cas échéant tenus à un secret professionnel ou à une obligation de confidentialité peuvent échanger avec l'administration pénitentiaire les informations indispensables lorsqu'il est dans l'intérêt du détenu concerné, des autres détenus, du personnel ou de la sécurité, de la salubrité du centre pénitentiaire ou des autres personnes ayant des contacts physiques avec les détenus, y compris en ce qui concerne la lutte contre des maladies contagieuses ».

Dans le projet de loi relatif à la loi du 20 juillet 2018 portant réforme de l'administration pénitentiaire les auteurs du projet de loi avaient relevé que lesdites dispositions légales visaient à « conférer une valeur légale au droit du détenu de bénéficier des soins dont il a besoin conformément à son état de santé physique et psychique » et à créer « une base légale permettant un meilleur échange d'informations cette fois-ci entre les médecins et les autres intervenants le cas échéant tenus à un secret professionnel ou une obligation de confidentialité et l'administration pénitentiaire. (...) le paragraphe 4 sous examen prévoit une disposition légale visant à permettre aux acteurs impliqués de mieux communiquer entre eux et de s'échanger les informations nécessaires aux meilleurs soins du détenu/patient. (...) Il est important de relever à cet égard qu'il n'est en aucune manière question d'imposer un échange d'in-

formations à qui que ce soit mais au contraire de créer une base légale visant à permettre un échange d'informations lorsque leur détenteur est persuadé qu'un échange est propice à la santé du détenu/de son patient. La formulation „Sans préjudice du secret professionnel ...“ vise donc à souligner que les acteurs impliqués ne sont pas déliés de leurs obligations de secret et/ou de confidentialité, mais qu'ils sont autorisés et encouragés à rechercher par exemple plus activement le consentement de leur patient afin d'échanger des informations »³¹⁶.

Dès lors, dans une telle hypothèse les traitements de données relatifs aux « informations contenues dans les bilans de suivi psychologique, psychosocial et psychothérapeutique des détenus » devraient se faire en conformité avec les dispositions de l'article 26, paragraphe (4) de la loi précitée.

En tout état de cause, la Commission nationale estime que l'administration pénitentiaire ne devrait pas avoir accès à l'ensemble des informations contenues dans le dossier médical et donc à l'ensemble des « informations contenues dans les bilans de suivi psychologique, psychosocial et psychothérapeutique des détenus ».

En effet, l'accès à de telles données devrait être limité aux « informations indispensables lorsqu'il est dans l'intérêt du détenu concerné, des autres détenus, du personnel ou de la sécurité, de la salubrité du centre pénitentiaire ou des autres personnes ayant des contacts physiques

³¹⁶ Document parlementaire n°7042//00, Ad article 26, pp. 39 à 41.

avec les détenus, y compris en ce qui concerne la lutte contre des maladies contagieuses ».

ii. Sur les informations contenues dans les rapports d'expertise

La CNPD comprend que les rapports d'expertise seraient transmis par le procureur général d'Etat à l'administration pénitentiaire afin de permettre à cette dernière de disposer des informations qui lui sont nécessaires pour l'exécution de ses missions.

En effet, les auteurs du projet de loi N°7042 portant réforme de l'administration pénitentiaire avaient précisé à ce sujet que les informations contenues dans les rapports d'expertise relatifs à la santé physique et psychique du détenu constituent « *des informations indispensables pour l'administration pénitentiaire afin qu'elle puisse remplir ses missions à l'égard de ce détenu conformément notamment à l'article 1^{er} paragraphe 2 et à l'article 3 paragraphes 3 et 4* »³¹⁷.

Sans préjuger de la nécessité de transmettre de telles informations, il y a lieu de s'interroger sur la conservation et l'accès ultérieur de telles données au sein de l'administration pénitentiaire alors qu'il ressort de l'article 130 du projet de règlement grand-ducal que ces dernières auraient vocation à être conservées dans le dossier d'insertion sociale de chaque détenu.

La CNPD y reviendra infra aux points III et IV du présent avis.

iii. Remarques finales

Il y a lieu de relever que l'article 44 du règlement grand-ducal du 24 mars 1989 concernant l'administration et le régime interne des établissements pénitentiaires, qui sera abrogé par le projet de règlement grand-ducal, dispose que le dossier individuel du détenu « *comprend les documents relatifs à la santé physique et mentale du détenu conservés dans une farde séparée à l'infirmerie* » et que « *[l]a partie médicale du dossier est adressée sous pli fermé au médecin de l'établissement de destination* ».

Dans la mesure où les dispositions précitées de l'article 44 du règlement grand-ducal du 24 mars 1989 concernant l'administration et le régime interne des établissements pénitentiaires ne sont pas reprises par le projet de règlement grand-ducal, la CNPD estime que de telles mesures devraient figurer dans le dispositif légal sous avis et rester d'application.

Ainsi, la Commission nationale se demande si les « *informations contenues dans les bilans de suivi psychologique, psychosocial et psychothérapeutique des détenus* » doivent à la fois figurer dans le dossier individuel et dans le dossier d'insertion sociale, qui sont deux registres différents, l'un tenu au greffe du centre pénitentiaire et l'autre tenu au service psycho-social et socio-éducatif.

Ne serait-il pas pertinent, compte tenu de la nature des données en cause, que de telles

³¹⁷ Document parlementaire n°7042/00, Ad article 18, page 33.

6

ANNEXES

informations figurent uniquement dans le dossier médical du détenu et soient aux mains du professionnel de santé concerné ?

C. Sur les « informations contenues dans le casier judiciaire du détenu »

L'article 127, paragraphe (1), point 14° du projet de règlement grand-ducal dispose que l'administration pénitentiaire peut traiter « les informations contenues dans le casier judiciaire du détenu ».

Pour une meilleure compréhension des données visées par les dispositions précitées, il conviendrait de préciser quel numéro de bulletin est visé et de se référer expressément à l'un des bulletins visés par la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire, alors 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 ladite loi.

Par ailleurs, il conviendrait de veiller à la bonne articulation entre les dispositions sous avis avec celles de l'article 17, paragraphe (2), de la loi du 20 juillet 2018 portant réforme de l'administration pénitentiaire.

En effet, ledit article dispose que « [p]ar dérogation à l'article 6 de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire, le bulletin n°1 du casier judiciaire est délivré sur demande motivée à l'administration

pénitentiaire pour tous les détenus. En ce qui concerne les détenus ressortissants d'un autre État membre de l'Union européenne ou d'un État tiers, l'administration pénitentiaire peut adresser une demande motivée au procureur général d'État en vue de l'obtention d'un extrait du casier judiciaire de l'autorité compétente de l'État membre dont le détenu concerné a la nationalité.

Sur demande motivée, l'administration pénitentiaire peut solliciter auprès du procureur général d'État copie des arrêts et jugements rendus antérieurement en matière pénale à l'égard d'un détenu par les juridictions nationales, ainsi que par les juridictions d'un autre État membre de l'Union européenne ou d'un État tiers. ».

II. Sur les registres visés par le projet de règlement grand-ducal

Comme énoncé supra au point I.1. du présent avis, le projet de règlement grand-ducal prévoit la tenue de 6 registres, à savoir :

- le registre d'admission ;
- le dossier individuel ;
- le dossier d'insertion sociale ;
- le registre des fouilles ;
- le registre visé à l'article 123 du projet de règlement grand-ducal ; et
- le registre des visites.

Il y a lieu de féliciter les auteurs du projet de règlement grand-ducal pour avoir précisé pour chacun des registres quelles données à caractère personnel y figureraient.

De même qu'il convient de saluer les auteurs du projet de loi pour avoir précisé aux articles 128 et 129 que le registre d'admission ainsi que le dossier individuel de chaque détenu sont tenus au greffe du centre pénitentiaire.

L'article 130 précise que le dossier d'insertion sociale de chaque détenu est tenu au service psycho-social et socio-éducatif.

De telles précisions mériteraient également d'être apportées pour le registre des fouilles, le registre visé à l'article 123 du projet de règlement grand-ducal ainsi que le registre des visites.

Par ailleurs, il est encore précisé que le registre des admissions, le dossier individuel et le dossier d'insertion sociale précité sont susceptibles d'être tenus sous forme électronique³¹⁸. A ce sujet, les auteurs du projet de règlement grand-ducal précisent notamment que ces registres peuvent être tenus sous forme électronique afin « *d'utiliser de manière optimale les nouvelles technologies disponibles* ».

En l'absence de précision dans le projet de règlement grand-ducal et dans le commentaire des articles quant aux modalités de la tenue de tels registres électroniques, la Commission nationale n'est pas en mesure d'apprécier les éventuelles problématiques relatives à la protection des données qui pourraient, le cas échéant, naître dans ce contexte.

Enfin, en l'absence de précisions à ce sujet dans le dispositif sous avis, il y a lieu de se demander si de telles mesures s'appliqueraient le cas échéant au registre des fouilles, au registre visé à l'article 123 du projet de règlement grand-ducal ainsi qu'au registre des visites.

III. Sur l'accès aux données collectées par l'administration pénitentiaire et sur la sécurité des traitements

Conformément au principe d'intégrité et de confidentialité, les données doivent être traitées de « *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* »³¹⁹.

Le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque³²⁰, notamment en ce qui concerne le traitement portant sur des catégories particulières de données à caractère personnel³²¹.

Pareilles mesures doivent être mises en œuvre afin d'éviter notamment des accès non autorisés aux données, des fuites de données ou des modifications non désirées.

³¹⁸ Voir articles 128, paragraphe (3), 129, paragraphe (2) et 130, paragraphe (2) du projet de règlement grand-ducal.

³¹⁹ Article 5, paragraphe (1), lettre f) du RGPD et article 3, paragraphe (1), lettre f) de la loi du 1^{er} 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.

³²⁰ Article 32 du RGPD et article 28, paragraphe (1) de la loi du 1^{er} 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.

³²¹ Article 28, paragraphe (1) de la loi du 1^{er} 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.

6

ANNEXES

Il y a lieu de féliciter les auteurs du projet de règlement grand-ducal d'avoir prévu à l'article 127, paragraphe (2) du projet de règlement grand-ducal que « *l'accès des membres de l'administration pénitentiaire aux données personnelles visées au paragraphe 1^{er} est strictement limité à ceux qui justifient d'un intérêt professionnel les obligeant à traiter ces données afin d'accomplir les missions prévues à l'article 3 de la loi du 20 juillet 2018 portant réforme de l'administration* ».

En effet, 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. Dans ce contexte, il est vivement recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début la personne ou le service compétent qui aurait accès aux données, et à quelles données précises cette personne ou ce service aurait accès. Ce d'autant plus dans la mesure où des catégories particulières de données seraient amenées à être traitées.

Le responsable du traitement devra ainsi mettre en place de telles mesures 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 outre, si des registres électroniques devaient être tenus, et si de tels traitements

tombent dans le champ d'application de la loi du 1^{er} août 2018 relative aux traitements de données en matière pénale ainsi qu'en matière de sécurité nationale, le responsable du traitement devrait veiller au respect des dispositions de l'article 28, paragraphe (2) et l'article 24 de la loi précitée.

L'article 24 de la loi précitée exige notamment que le responsable du traitement définisse les profils et modalités d'accès et procéder à des vérifications régulières des logues à des fins, notamment, « *d'autocontrôle [et] de garantie de l'intégrité et de la sécurité des données à caractère personnel* ». Dans de tels cas, le responsable de traitement devrait donc procéder à des revues de logues régulières et proactives, notamment en lien avec les mesures et procédures à mettre en place pour tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement conformément à l'article 28 de ladite loi.

IV. Sur la durée de conservation des données

Conformément au principe de la limitation de la conservation, 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* »³²².

S'il y a lieu de féliciter les auteurs du projet de règlement grand-ducal d'avoir prévu à l'article

³²² Article 5, paragraphe (1), lettre e) du RGPD et article 3, paragraphe (1), lettre e) de la loi du 1^{er} 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.

132 qu' « [à] la libération du détenu, les dossiers prévus aux articles 129 et 130 sont classés dans les archives du greffe pour y être conservés pour une durée maximale de trente ans » et qu'en « cas de nouvelle détention intervenant dans le délai visé au paragraphe 1^{er}, les dossiers sont reproduits pour être continués. En l'absence d'une nouvelle détention dans ce délai, les données sont détruites ou anonymisées pour être utilisées à des fins statistiques ou historiques ».

Elle regrette cependant que les critères justifiant une telle durée ne soient pas précisés dans le commentaire des articles, de sorte qu'elle n'est pas en mesure d'apprécier si une telle durée apparaît proportionnée en l'espèce.

Ainsi décidé à Belvaux en date du 1^{er} octobre 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7897 portant modification: 1° de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 ; 2° de la loi modifiée du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière ; 3° de la loi modifiée du 22 janvier 2021 portant : 1° modification des articles L. 234-51, L. 234-52 et L. 234-53 du Code du travail ; 2° dérogation temporaire aux dispositions des articles L. 234-51, L. 234-52 et L. 234-53 du Code du travail. (Délibération n° 34/AV28/2021 du 12/10/2021

Conformément à l'article 57, paragraphe 1^{er}, lettre (c) du règlement (UE) 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 1^{er} 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 courriel en date du 8 octobre 2021, Madame la Ministre de la Santé a invité la Commission

nationale à se prononcer sur le projet de loi n° 7897 portant modification: 1° de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 ; 2° de la loi modifiée du 8 mars 2018 relative aux établissements hospitaliers et à la planification hospitalière ; 3° de la loi modifiée du 22 janvier 2021 portant : 1° modification des articles L. 234-51, L. 234-52 et L. 234-53 du Code du travail ; 2° dérogation temporaire aux dispositions des articles L. 234-51, L. 234-52 et L. 234-53 du Code du travail (ci-après le « projet de loi n° 7897 »).

D'après l'exposé des motifs, le projet de loi n° 7897 « *se propose d'apporter quelques adaptations ponctuelles à la version actuelle de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 qui vient à échéance le 18 octobre 2021.* »

La CNPD constate dans ce contexte que le nouveau paragraphe (2) de l'article 2 du projet de loi n° 7897 prévoit que dorénavant à l'intérieur des établissements de restauration et de débit de boissons, les clients et l'ensemble du personnel de l'établissement concerné sont obligatoirement soumis au régime Covid check,³²³ tandis que l'article 3septies dudit projet accorde la faculté à tout chef d'entreprise ou chef d'administration de placer l'ensemble ou une partie seulement de son entreprise ou de son administration sous le régime Covid check afin de protéger la sécurité et la santé des travailleurs concernés.

Les clients, voire les employés concernés en cas de choix du régime Covid check par

³²³ Voir la nouvelle définition du « régime Covid check » prévue à l'article 1^{er}, point 27 du projet de loi n° 7897.

l'employeur, sont donc obligés de présenter un certificat de vaccination, de rétablissement ou de test Covid-19 indiquant un résultat négatif tel que visé aux articles 3bis, 3ter ou 3quater du projet de loi n° 7897. Néanmoins, il ne ressort pas clairement dudit projet de loi, ni du commentaire des articles, si des traitements de données à caractère personnel seraient effectués par l'employeur ou l'exploitant des établissements de restauration et de débit de boissons, suite à la présentation par un client ou un employé d'un tel certificat.

L'employeur ou l'exploitant collectera-t-il ou enregistrera-t-il les données figurant sur lesdits tests ou lesdits certificats suite à leur présentation ? En effet, un employeur, comment pourra ou devra-t-il gérer le régime Covid Check au quotidien en pratique d'un point de vue protection des données à caractère personnel ? Soumettra-t-il tous les salariés quotidiennement à un contrôle Covid Check ou pour des raisons pratiques tiendra-t-il un fichier avec les données des salariés qui sont vaccinés ou rétablis. Le projet de loi ne donne pas de réponse à ces questions et manque de précision à ce sujet.

Il y a lieu de rappeler par ailleurs que le RGPD n'aura vocation à s'appliquer que lorsqu'un traitement de données à caractère personnel sera effectué³²⁴, par exemple si le fait qu'un employé ou client a présenté un résultat de test antigénique rapide certifié, un certificat de vaccination ou un certificat de test de dépistage sérologique est amené à être consigné dans un fichier par l'employeur ou l'exploitant.

En outre, dans l'hypothèse où des traitements de données seraient effectués dans le cadre du projet de loi n° 7897, ceux-ci doivent reposer sur une des bases de licéité énumérée à l'article 6 du RGPD ainsi que respecter l'une des conditions visées à l'article 9, paragraphe (2), du RGPD dans la mesure où des données relatives à la santé des personnes concernées seraient susceptibles d'être traitées.

A ce titre, il y a lieu de rappeler que le traitement de données à caractère personnel collectées et traitées en vertu d'une obligation légale doit reposer sur une base légale conformément à l'article 6, paragraphe (3), du RGPD, lu ensemble avec son paragraphe (1), lettres c). Conformément à l'article 6, paragraphe (3), du RGPD cette obligation légale devrait définir les finalités du traitement et 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* ».

Le considérant 41 du RGPD précise encore que cette mesure législative devrait être

³²⁴ Voir la définition d'un traitement de données à caractère personnel prévue à l'article 4.2 du RGPD.

6

ANNEXES

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'homme³²⁵.

Or, force est de constater que si des traitements de données devaient être effectués sur base du projet de loi n° 7897, ceux-ci ne pourraient valablement reposer sur une telle base de licéité alors que le dispositif sous avis ne respecte pas les exigences juridiques exposées ci-avant.

En considération des observations qui précèdent, la Commission nationale considère que dans l'hypothèse où des traitements de données seraient effectués par les organismes concernés, le texte 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'homme³²⁶, et ne peut, dès lors, se prononcer plus en détail sur les éventuels aspects qui seraient liés à la protection des données personnelles.

En ce qui concerne plus spécifiquement le régime du Covid check, la CNPD comprend qu'après avoir scanné le code QR du certificat CovidCheck, le résultat s'affiche instantanément : l'écran est vert si le certificat est valide et rouge dans le cas contraire. Toutefois, il s'avère que d'autres informations complémentaires s'affichent également sur l'écran lors du contrôle.

Par exemple, dans le cas d'une personne vaccinée, il s'agit des informations suivantes : les nom et prénoms de la personne concernée, sa date de naissance, la référence à la maladie ou le virus Covid-19, la dénomination du vaccin, le titulaire de l'autorisation de mise sur le marché ou le fabricant du vaccin, la date de la vaccination, l'Etat dans lequel le vaccin a été administré, l'émetteur du certificat et son identifiant.

Conformément à l'article 5, paragraphe 1, lettre c) du RGPD, les données à caractère personnel doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)* ». En outre, tout traitement de données à caractère personnel doit être nécessaire et proportionné à la finalité poursuivie par ledit traitement.

Bien que la CNPD comprend que l'application CovidCheck.lu a pour objectif de simplifier les vérifications des certificats, la CNPD s'interroge sur la nécessité de rendre visible l'ensemble des informations susmentionnées, systématiquement lors de chaque contrôle. En effet, il semble que le même objectif pourrait être atteint en affichant simplement l'état du certificat CovidCheck (valide – vert ; invalide – rouge). Par ailleurs, un employeur ou un restaurateur peut-il valider un certificat en lisant les informations qui accompagnent le code QR, si par exemple l'application est indisponible, s'il n'y a pas de réception réseau ou si l'appareil pour le scan ne fonctionne plus ?

³²⁵ 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. Voir entre autres CourEDH, Zakharov e. Russie [GCL n°47413/06], § 228-229, 4 décembre 2015, CourEDH, Vavříčka et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.

³²⁶ 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, CourEDH, Vavříčka et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.

Les conditions générales d'utilisation de l'application CovidCheck disponibles sur le site <https://covid19.public.lu/covidcheck> précisent en outre que les plateformes Apple App Store et Google Play Store sont susceptibles de traiter les données à caractère personnel communiquées directement ou indirectement par l'utilisateur dans le cadre du téléchargement de l'application. Il y a ainsi lieu de souligner qu'au regard du fait que l'application CovidCheck contient des données concernant la santé, il est important d'être particulièrement vigilant à utiliser des mesures techniques et organisationnelles adéquates conformément aux articles 25 paragraphe (2) et 32 paragraphe (1) du RGPD afin que celles-ci ne puissent pas être accessibles aux personnes non autorisées.

Finalement, bien que ces problématiques ne relèvent pas du domaine de la protection des données, la CNPD s'était déjà interrogée en termes de droit du travail dans ses avis du 28 mai 2021³²⁷ et du 8 juin 2021³²⁸ sur les conséquences d'un refus par un employé de se soumettre à l'obligation de présenter un des

certificats mentionnés aux articles 3bis, 3ter ou 3quater du projet de loi n° 7897. La même question se pose également pour les salariés qui ne sont ni vaccinés, ni rétablis. Devront-ils tous les deux jours présenter un test Covid-19 certifié indiquant un résultat négatif pour pouvoir travailler ?

Ainsi décidé à Belvaux en date du 12 octobre 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

³²⁷ Délibération n° 20/AV16/2021 du 28/05/2021 : <https://cnpd.public.lu/fr/decisions-avis/20201/20-AV16-PL7808-depistage-covid19.html>.

³²⁸ Délibération n° 24/AV19/2021 du 8 juin 2021 : <https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2021/24-AV19-2021-du-8-juin-2021-PL-7836-Covid.pdf>

6

ANNEXES

**Avis de la Commission nationale pour la protection des données relatif aux amendements à la proposition de révision du chapitre II de la Constitution (numéro de dossier parlementaire : 7755).
(Délibération n°48/AV29/2021 du 29/10/2021)**

Conformément à l'article 57, paragraphe 1^{er}, lettre (c) du règlement (UE) 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 1^{er} 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 17 août 2021, Monsieur le Ministre d'Etat a invité la Commission nationale à se prononcer sur les amendements à la proposition de révision du chapitre II de la Constitution (ci-après la « proposition de révision »).

La proposition de révision représente une partie de la révision de la Constitution par

étapes et porte sur le chapitre II dédié aux droits et libertés.

L'article 24 de la proposition de révision

La CNPD n'a pas d'observation à formuler concernant les amendements à la révision du chapitre II. Elle aimerait cependant attirer l'attention sur l'article 24 de la proposition de révision, article ne faisant pas l'objet d'un amendement.

Cet article prévoit un droit à la protection des données selon les termes suivants : « *Toute personne a droit à l'autodétermination informationnelle et à la protection des données à caractère personnel la concernant. Ces données ne peuvent être traitées qu'à des fins et dans les conditions déterminées par la loi.* »

Selon le commentaire des articles, l'article 24 de la proposition de la révision s'inspire de l'article 8 de la Charte des droits fondamentaux de l'Union européenne qui dispose ce qui suit :

« *Protection des données à caractère personnel*

1. *Toute personne a droit à la protection des données à caractère personnel la concernant.*
2. *Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.*
3. *Le respect de ces règles est soumis au contrôle d'une autorité indépendante.* »

Il convient de relever que les dispositions de la Charte s'adressent aux « États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union » (article 51 de la Charte). Il s'en suit que certains domaines sont exclus du champ d'application de la Charte au niveau national³²⁹, ce qui rend l'introduction de la protection des données dans la constitution luxembourgeoise d'autant plus positive.

La deuxième phrase de l'article 24 projeté et le deuxième paragraphe de l'article 8 de la Charte des droits fondamentaux de l'Union européenne diffèrent de par leurs formulations, leurs sens et de leurs conséquences juridiques qui s'en suivent. La deuxième phrase de l'article 24 projeté impliquerait, en effet, d'après la compréhension de la CNPD que chaque finalité pour laquelle des données à caractère personnel sont traitées par un responsable du traitement devrait être prévue par une loi. La Commission nationale s'interroge dès lors sur les intentions des auteurs et les raisons de la formulation de cette disposition. Dans un souci de sécurité juridique et pour éviter tous doutes relatifs à l'interprétation constitutionnelle en projet, la CNPD recommande fortement que le libellé s'aligne sur celui de l'article 8 de la Charte.

Droit comparé

Allemagne

En date du 15 décembre 1983, dans son célèbre « Volkszählungsurteil », la cour constitutionnelle allemande a établi le principe de l'autodé-

termination informationnelle (« *informationelle Selbstbestimmung* »).

Pour cela, la Cour s'est basée sur l'inviolabilité de la dignité humaine de l'article 1^{er} de la constitution allemande et le droit au développement de la personnalité (« *freie Entfaltung der Persönlichkeit* ») prévue par l'article 2 de la Constitution.

Ce droit à l'autodétermination informationnelle a été confirmé par des arrêts ultérieurs.

Cependant, à ce jour, il n'a pas été introduit de manière explicite dans la constitution fédérale allemande.

En revanche, aujourd'hui, un droit à la protection des données est prévu de manière explicite par les constitutions de certains Länder.

A titre d'exemple, on peut mentionner :

- l'article 4 paragraphe (2) de la constitution du Land de Rhénanie-Palatinat :

« (1) *Jeder Mensch hat das Recht, über die Erhebung und weitere Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen. Jeder Mensch hat das Recht auf Auskunft über ihn betreffende Daten und auf Einsicht in amtliche Unterlagen, soweit diese solche Daten enthalten.*

(2) *Diese Rechte dürfen nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt*

³²⁹ Voir à ce sujet: fiche thématique « CHAMP D'APPLICATION DE LA CHARTE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE », Cour de justice de l'Union européenne, Direction de la Recherche et de la documentation
https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_fr.pdf

6

ANNEXES

werden, soweit überwiegende Interessen der Allgemeinheit es erfordern.»

- l'article 4 paragraphe (2) de la constitution du Land de Rhénanie-du-Nord-Westphalie :

« (2) Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Eingriffe sind nur in überwiegendem Interesse der Allgemeinheit auf Grund eines Gesetzes zulässig.»

- l'article 12a de la constitution du Land de Hesse:

« Jeder Mensch ist berechtigt, über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst zu bestimmen. ²Die Vertraulichkeit und Integrität informationstechnischer Systeme werden gewährleistet. ³Einschränkungen dieser Rechte bedürfen eines Gesetzes.»

France

En France, le Conseil constitutionnel a, en 2012, posé le principe selon lequel « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à l'objectif poursuivi »³³⁰.

Pour cela, le Conseil constitutionnel s'est basé sur le droit à la liberté personnelle garanti par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 ainsi

que le droit au respect de la vie privée qui en découle.

Le principe établi par l'arrêt de 2012 a été confirmé par des arrêts ultérieurs du Conseil constitutionnel³³¹.

La Constitution ne prévoit, à ce jour, pas de droit explicite à la protection des données.

Belgique

La Cour constitutionnelle belge a pris un certain nombre de décisions tendant à garantir la protection des données en se basant sur le droit au respect de la vie privée prévu par l'article 22 de la Constitution belge.

La Constitution ne mentionne cependant pas la protection des données ou le droit à l'autodétermination informationnelle de manière explicite.

Conclusion

La CNPD se félicite de l'introduction de la protection des données dans la Constitution, qui démontre ainsi l'intention de consacrer ce principe au rang le plus élevé de la hiérarchie des normes juridiques luxembourgeoises, y compris pour des matières ne relevant pas du champ d'application de la Charte des droits fondamentaux de l'Union européenne. Cette intention présente un caractère précurseur, alors qu'il n'est pas consacré aussi explicitement dans les Constitutions des pays voisins, même si l'interprétation qu'en

³³⁰ Décision n° 2012-652 DC du 22 mars 2012, considérant 8 : <https://www.conseil-constitutionnel.fr/decision/2012/2012652DC.htm>

³³¹ Par exemple:

- Décision n° 2013-681 DC du 05 décembre 2013, considérant 27 : <https://www.conseil-constitutionnel.fr/decision/2013/2013681DC.htm>

- Décision n° 2014-690 DC du 13 mars 2014, considérant 51 : <https://www.conseil-constitutionnel.fr/decision/2014/2014690DC.htm>

tirent les hautes juridictions précitées vont dans le même sens.

Ainsi décidé à Belvaux en date du 29 octobre 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7674 portant organisation de l'accès à la connaissance de ses origines dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs. (Délibération n°52/AV30/2021 du 29/11/2021)

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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* ».

N'ayant pas été directement saisie par Madame la Ministre de la Justice, ni au stade de l'avant-projet, ni au stade du projet de loi, la Commission nationale souhaite néanmoins se prononcer quant au projet de loi n°7674 portant organisation de l'accès à la connaissance de ses origines dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs (ci-après le « *projet de*

loi »), tel qu'amendé en date du 4 mai 2021, et quant aux interactions de ce dernier avec le cadre légal relatif à la protection des données à caractère personnel. Le présent avis suit le texte coordonné tel qu'amendé³³².

L'autosaisine de la Commission nationale intervient dans le cadre des nombreux traitements de données à caractère personnel, entre autres de données de santé, réalisés aux fins de l'exercice de l'accès à la connaissance de ses origines et affectant les aspects les plus intimes de la vie privée des personnes concernées.

Bien que la Commission nationale ne souhaite nullement remettre en cause la légitimité des nouvelles mesures introduites par le projet de loi, elle souligne cependant que des garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données à caractère personnel doivent être mises en œuvre. La Commission nationale soulève dès lors la nécessité de prévoir des mesures juridiques, organisationnelles et techniques afin d'assurer un haut niveau de protection des données à caractère personnel.

I. Observations transversales

A. Remarques liminaires

A titre liminaire, il y a lieu de soulever une question quant au champ d'application du projet de loi sous avis. En effet, les titres du second chapitre, et en particulier celui de la première section de ce chapitre, incitent à

³³² Document parlementaire N°7674/02.

penser que seuls les enfants nés sous secret qui seront par la suite adoptés auraient le droit à connaître leurs origines, tandis que des enfants nés sous secret, et qui ne feront pas l'objet d'une adoption, ne disposeraient pas de ce droit. Cette interprétation est confortée par l'intitulé du projet de loi ainsi que par l'article 4, paragraphe 3, qui dispose que « *[l]e traitement de ces données est nécessaire aux fins de la mise en œuvre de la recherche de l'accès d'un enfant à ses origines dans le cadre de l'adoption ou d'une procréation médicalement assistée avec tiers donneurs* ».

Or, la CNPD ne perçoit pas la raison de cette différence de traitement, d'autant plus qu'il est impossible de savoir au moment de l'accouchement si l'enfant fera l'objet d'une adoption. Une telle distinction aurait pour conséquence que les enfants nés sous secret et qui ne sont pas adoptés par la suite n'ont pas le droit de se voir communiquer les informations qui ont été collectées à leur propos en application du projet de loi.

De plus, le projet de loi n°6568A portant réforme de la filiation tel qu'amendé ne prévoit pas une telle différence de traitement dans la mesure où le nouvel article 312bis du Code civil dispose que « *[l]'enfant a le droit d'avoir, dans la mesure du possible, accès à ses origines. [...]* ». Le commentaire des articles précise que « *[l]es dispositions de cet article sont applicables qu'il s'agisse d'accès aux données relatives aux origines d'une personne en cas d'accouchement sous X, d'adoption plénière, de procréation médicalement assistée*

ou de gestation pour autrui ». Une attention particulière devra partant être accordée à l'articulation du projet de loi sous avis avec le projet de loi n°6568A.

Encore à titre liminaire, il convient de clarifier que le droit d'accès aux origines d'un enfant, ne doit pas être confondu avec le droit d'accès de la personne concernée à des données personnelles le concernant tel que prévu à l'article 15 du RGPD. A ce titre, il y a lieu de rappeler que le droit d'accès au sens de l'article 15 du RGPD confère aux personnes concernées le droit de s'adresser directement au responsable du traitement afin de demander confirmation que des données à caractère personnel le concernant sont ou ne sont pas traitées. Ce même droit confère à la personne concernée d'obtenir une copie des données à caractère personnel faisant l'objet d'un traitement, pour autant que cette copie ne porte pas atteinte aux droits et libertés d'autrui (limitation prévue à l'article 15, paragraphe 4 du RGPD). A titre d'exemple, un enfant concerné pourrait exercer son droit d'accès sur base de l'article 15 du RGPD auprès de l'hôpital dans lequel il est né. L'hôpital en question est dès lors tenu, en prenant en compte les éventuelles limitations prévues à l'article 15 du RGPD, à communiquer à l'enfant l'intégralité des données le concernant. Or, cet exercice du droit d'accès sur base de l'article 15 du RGPD ne doit pas être confondu avec l'exercice du droit d'accès à ses origines qu'entend mettre en place le présent projet de loi en ce que ce dernier droit d'accès s'adresse à un autre responsable du traitement (le ministre en

6

ANNEXES

l'occurrence) et ne pourra guère être limité tel que le droit d'accès prévu par le RGPD (pas de copie si la demande porte atteinte aux droits et libertés d'autrui - article 15, paragraphe 4 du RGPD).

Par ailleurs, l'article 1^{er} du projet de loi prévoit que « *l'accès à ses origines ne fait naître ni droit ni obligation au profit ou à la charge de qui que ce soit* ». Cette disposition est particulièrement ambiguë, étant donné que l'objectif du projet de loi est précisément d'instaurer le droit à l'accès à ses origines. Il crée également des obligations, telles que par exemple à l'article 20 qui prévoit, dans le cadre de la procréation médicalement assistée avec tiers donneurs (ci-après « *la PMA* »), l'obligation pour les auteurs du projet parental de procéder à la déclaration spontanée de certaines informations au ministre ayant dans ses attributions le projet de loi (ci-après le « *ministre* »). La Commission nationale estime, au regard du commentaire des articles, qu'il était dans l'intention des auteurs du projet de loi de ne pas créer des obligations et droits en matière de filiation. Elle se rallie dès lors à la suggestion émise par le Conseil d'Etat dans son avis du 16 juillet 2021³³³ de supprimer cet article.

B. Quant à l'article 6, paragraphe 3, du RGPD

Selon l'article 6, paragraphe 1^{er} du RGPD, un traitement n'est licite que si au moins une des conditions y énumérées est remplie. La Commission nationale comprend que le projet de loi sous avis entend créer une condition de licéité au sens de l'article 6, paragraphe 1^{er}

lettre c) du RGPD, à savoir que le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.

Or, l'article 6, paragraphe 3 du RGPD dispose que « *[l]e fondement du traitement visé au paragraphe 1, points c) et e), est défini par:*

1. *le droit de l'Union; ou*
2. *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 situa-

³³³ Avis n°60.376 du 16 juillet 2021 du Conseil d'Etat sur le projet de loi portant organisation de l'accès à la connaissance de ses origines dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs, p.4.

tions particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi. »

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'Etat 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 Etat 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 énonce encore que « [l]orsque 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 ».

Bien que le projet de loi fournisse une base légale pour les traitements en cause en spécifiant un certain nombre d'éléments, tels que les finalités des traitements ou encore la durée de conservation des données, certains points ne sont pas suffisamment précisés dans le projet de loi.

La CNPD reviendra ultérieurement sur ce point mais tient d'ores et déjà à soulever la mention, dans la fiche financière du projet sous avis, de la création d'un « outil informatique pour la sauvegarde des données à caractères confidentielles hautement sensibles ». En effet, ni le projet de loi lui-même, ni l'exposé des motifs ne font référence à cet outil informatique.

Il y a, dès lors, lieu de s'interroger sur son utilisation dans le cadre de l'exercice de l'accès aux origines, en particulier en ce qui concerne un éventuel traitement des données à caractère personnel effectué à l'aide de cet outil. Quelles données sont appelées à figurer dans cet outil ? Comment cet outil est-il

6

ANNEXES

alimenté ? Dans le cadre de l'accouchement sous secret notamment, est-ce que cela signifie qu'une personne habilitée ouvre les plis reçus pour insérer ensuite les informations dans l'outil informatique ? Quel est ensuite le sort du support physique ? Est-ce que des sous-traitants agissent dans l'exploitation et la gestion de cet outil ? Il conviendrait de répondre à ces différentes questions dans le texte du projet de loi. Des mesures de sécurité techniques et organisationnelles appropriées et adaptées aux risques, compte tenu de la sensibilité des données, devront en tout état de cause être mises en place par le ou les responsables de traitement conformément à l'article 32 du RGPD. En outre, en cas de recours à des sous-traitants, les obligations qui incombent tant au responsable du traitement qu'aux sous-traitants en application des articles 28 et 29 du RGPD auront vocation à s'appliquer.

II. Quant aux rôles des différents intervenants

Bien qu'il y ait lieu de féliciter les auteurs du projet de loi d'avoir pris le soin de déterminer le ministre comme responsable du traitement³³⁴, des imprécisions quant aux rôles des différents intervenants subsistent.

En effet, il ressort du commentaire des articles que les établissements hospitaliers jouent un rôle important lors des accouchements sous secret dans la mesure où ils constituent le plus souvent « *le premier et le seul contact des futures mères en cause* »³³⁵.

Ainsi, l'article 5 du projet de loi dispose que l'établissement hospitalier doit informer le ministre de l'accouchement sous secret et fournir aux parents de naissance un certain nombre d'informations. Les mêmes obligations incombent à tout autre professionnel encadrant la naissance qui a lieu dans un autre endroit qu'un établissement hospitalier.

En vertu de l'article 6 du projet de loi, il appartient à l'établissement hospitalier ou à tout autre professionnel ayant encadré la naissance de collecter un certain nombre d'informations concernant les parents de naissance et de les transmettre au ministre.

Dans le cadre des articles 16 et 17 qui traitent des « *autres adoptions nationales* » ainsi que des « *adoptions internationales* », d'autres acteurs sont appelés à fournir des informations à savoir les « *autorités judiciaires* », « *l'autorité centrale pour l'adoption au sens de la Convention de La Haye du 29 mai 1993 sur la protection des enfants et la coopération en matière d'adoption internationale, les organismes autorisés et habilités pour l'adoption conformément à la loi du 31 janvier 1998 portant agrément des services d'adoption et définition des obligations leur incombant* » et « *tout autre organisme ou autorité nationale intervenus dans le cadre de l'adoption* ».

Les articles 19 et 20 du chapitre 3 (l'accès à la connaissance de ses origines dans le cadre d'une procréation médicalement assistée avec tiers donneur) du projet de loi introduisent encore d'autres acteurs susceptibles à fournir

³³⁴ Article 4, paragraphe 1 du projet de loi.

³³⁵ Voir commentaire de l'article 5 du projet de loi.

des données à caractère personnel, à savoir les « auteurs du projet parental », les « centres de fécondation » ainsi que « tout médecin chargé de mettre en œuvre la procréation médicalement assistée ».

Si l'article 4, paragraphe 1^{er} du projet de loi détermine expressément le ministre comme responsable de traitement, il n'existe pas une telle clarté pour les autres acteurs. En effet les autres acteurs énoncés par le projet de loi, tel que par exemple l'établissement hospitalier ou tout autre professionnel ayant encadré la naissance dans le cadre de l'accouchement sous secret, voire pour la PMA les auteurs du projet parental ou les centres de fécondation, ou pour les autres adoption nationales et internationales les autorités judiciaires ou l'autorité centrale pour l'adoption, occupent un rôle primordial dans la collecte des données personnelles et leur transmission subséquente au responsable du traitement.

Or, il est important de déterminer dans le projet de loi le rôle des différents intervenants alors que les notions de « responsable du traitement », « responsable conjoint du traitement » et « sous-traitant » sont essentielles pour l'application du RGPD dans la mesure où elles déterminent qui est responsable du respect des règles relatives à la protection des données et comment les personnes concernées peuvent exercer leurs droits.

Le projet de loi devrait dès lors indiquer clairement si tous ces intervenants sont à considérer comme responsables du traitement

à part entier, responsables conjoints du traitement ou comme sous-traitants.

Par ailleurs, comme d'après la rédaction actuelle du texte le ministre est à considérer comme seul responsable du traitement, la Commission nationale se demande si ce constat implique qu'il y a création d'un fichier centralisé de données à considérer comme hautement sensibles. En effet, l'obligation qui incombe aux différents acteurs de fournir des informations au responsable du traitement implique que ceux-ci occupent une fonction de source d'information du ministre qui, pour sa part, conserve et gère les informations.

Dans ce contexte, il convient d'attirer l'attention des auteurs du projet de loi sur les lignes directrices élaborées par le Comité Européen de la Protection des Données qui sert de guidance aux acteurs dans la détermination de leurs rôles respectifs pour les traitements de données personnelles³³⁶.

III. Quant aux finalités

En vertu du principe de limitation des finalités prévu à l'article 5, paragraphe 1^{er}, lettre b), du RGPD, les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes ». Les objectifs poursuivis doivent être choisis et connus avant le début du traitement. De plus, ils doivent être définis de manière précise et se référer à un ou plusieurs buts précis (finalités déterminées et explicites).

³³⁶ Guidelines 07/2020 on the concepts of controller and processor in the GDPR (uniquement disponible en anglais).

6

ANNEXES

S'il y a lieu de féliciter les auteurs du projet de loi pour avoir précisé les finalités des traitements qui seraient mis en œuvre par le ministre à l'article 4, paragraphe 3, du projet de loi, les dispositions sont toutefois rédigées de manière trop vague en ce qu'elles se limitent à prévoir que « [l]e traitement de ces données est nécessaire aux fins de la mise en œuvre de la recherche de l'accès d'un enfant à ses origines dans le cadre de l'adoption ou d'une procréation médicalement assistée avec tiers donneurs ».

En effet, à la lecture du projet de loi, il y a lieu de constater que la recherche de l'accès d'un enfant à ses origines s'articule principalement autour de quatre objectifs :

- la constitution de dossiers par le ministre sur base d'informations reçues en vertu des articles 6, 10(3°), 10(4°), 10(5°), 20, 27 ou recherchées en vertu des articles 16, 17 et 25 paragraphe 3 ;
- la gestion par le ministre des demandes d'accès reçues par les enfants en vertu des articles 11 et 22 du projet de loi ;
- la gestion par le ministre des demandes du ou des parents de naissance s'enquérant de la recherche éventuelles par l'enfant en vertu de l'article 10 (6°) du projet de loi ;
- la communication aux enfants de leurs dossiers et/ou des informations collectées.

Ainsi, les dispositions de l'article 4, paragraphe 3 du projet de loi sont trop générales en ce qu'elles ne permettent pas de couvrir la pluralité des finalités des traitements qui

seraient mis en œuvre par le ministre dans le cadre du projet de loi.

Par exemple, et tel que relevé par le Conseil d'Etat, dans son avis du 16 juillet 2021, quant à aux dispositions de l'article 25, paragraphe (3), du projet de loi qui prévoient que le ministre peut consulter les archives de la juridiction ayant prononcé l'adoption ou si nécessaire consulter les dossiers de protections internationales s'il y a un indice que l'un ou les deux parents de naissance étaient bénéficiaires d'une telle protection, qu'une telle consultation « réside dans la recherche d'indices sur l'identité des parents de naissance. Le Conseil d'Etat considère que, dans une optique de protection des données, il s'agit d'une finalité qui doit être mentionnée dans le texte »³³⁷.

En outre, l'article 10 du projet de loi, points 9° et 10°, dispose que le ministre a pour mission de « gérer et traiter les informations recueillies » et « de revoir et de gérer les demandes d'accès à la connaissance de ses origines des personnes visées à l'article 11 ».

De plus, en vertu de l'article 21 point 3° du projet de loi, le ministre a encore pour mission « de recevoir, de gérer et de traiter les informations visées à l'article 20 ».

Or, en l'absence d'explications dans le commentaire des articles, il y a lieu de s'interroger sur les traitements de données personnelles qui seraient mis en œuvre dans le cadre de cette mission.

³³⁷ Voir observations formulées par le Conseil d'Etat au sujet de l'article 25 du projet de loi dans son avis n°60.376 du 16 juillet 2021 du Conseil d'Etat sur le projet de loi portant organisation de l'accès à la connaissance de ses origines dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs, p.14.

La Commission nationale se demande s'il ne serait pas opportun de clarifier les différents traitements de données qui seraient mis en œuvre par le ministre dans le cadre de ses missions, aussi dans un optique d'améliorer la sécurité juridique. Cela permettrait en effet d'améliorer la compréhension générale du projet de loi et de garantir la sécurité juridique.

Il résulte de ce qui précède qu'il ressort que la finalité décrite à l'article 4, paragraphe 3, du projet de loi paraît trop vague par rapport à l'exigence du RGPD de prévoir des finalités déterminées et explicites, surtout dans un domaine aussi sensible qu'est censé réglementer le projet de loi sous avis.

A toutes fins utiles, il ressort du commentaire des articles que l'article 4, paragraphe 5 du projet de loi vise à préciser les différentes obligations incombant au ministre en tant que responsable du traitement. Or, il convient de constater que l'énumération y faite se borne à recopier certains principes énumérés à l'article 5 du RGPD.

Dans son avis du 16 juillet 2021, le Conseil d'Etat relève, en effet, que « [l]e paragraphe 5 ne fait que rappeler les principes énoncés à l'article 5 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive

95/46/CE (règlement général sur la protection des données). Dès lors que ce règlement européen est d'application directe, la disposition sous revue est à supprimer. »³³⁸ La Commission nationale se rallie à l'observation du Conseil d'Etat.

IV. Quant aux catégories de données à caractère personnel

Il convient de relever que l'article 4 du projet de loi qui « constitue la base légale pour la gérance, la collecte et le traitement de données en cause »³³⁹ ne précise pas les catégories de données qui seraient collectées par le ministre « aux fins de la mise en œuvre de la recherche de l'accès d'un enfant à ses origines dans le cadre de l'adoption ou d'une procréation médicalement assistée avec tiers donneurs »³⁴⁰.

En outre, et comme relevé par le Conseil d'Etat, le paragraphe (4) de l'article 4³⁴¹ précité est superfluateur « [à] défaut d'énumérer les données traitées ou de renvoyer à la disposition précise qui énumère les données ».

En effet, il y a lieu de relever que les catégories de données qui seraient traitées à de telles fins résultent des dispositions des articles 6, 10, 11, 16, 17, 20, 22, 25, 26 et 27 du projet de loi.

Les articles 6, 10 et 11 font partie du Chapitre 2 « L'accès à la connaissance de ses origines dans le cadre d'une adoption », section 1^{ère} « L'adoption nationale », sous-section 1^{ère}

³³⁸ Avis n°60.376 du 16 juillet 2021 du Conseil d'Etat sur le projet de loi portant organisation de l'accès à la connaissance de ses origines dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs, p.5.

³³⁹ Voir commentaire des articles, article 4, page 15.

³⁴⁰ Article 4, paragraphe (3) du projet de loi.

³⁴¹ L'article 4, paragraphe (4) du projet de loi dispose que « [d]ans ce contexte sont traitées des données à caractère personnel qui sont visées par le présent projet de loi ».

6

ANNEXES

« L'accouchement sous secret », l'article 16 de la sous-section « Les autres adoptions nationales » et l'article 17 de la section 2 « L'adoption internationale » dudit chapitre.

Les articles 20 et 22 appartiennent au Chapitre 3 « L'accès à la connaissance de ses origines dans le cadre d'une procréation médicalement assistée avec tiers donneur » et les articles 25 à 27 font partie du Chapitre 5 « Dispositions transitoires et sur l'entrée en vigueur ».

Il serait en effet préférable, tel que suggéré par le Conseil d'Etat, de regrouper dans un seul article et d'énumérer en fonction des cas de figure (accouchement sous X, adoption nationale, adoption internationale, PMA), les catégories de données qui seraient traitées. Alternativement, il pourrait être envisagé de faire figurer une liste au début de chaque chapitre les catégories de données qui seraient traitées dans la mise en œuvre de ce chapitre.

A. Quant à l'article 9 du RGPD

Tout d'abord, il convient de relever que dans la mesure où une partie des données traitées par le responsable du traitement sont susceptibles d'être relatives à la santé des parents de naissance, pour les accouchements sous secret et les adoptions nationales et internationales, ou des tiers donneurs, pour les procréations médicalement assistées, celles-ci sont à qualifier de catégories particulières de données, dites « données sensibles », au sens de l'article 9 du RGPD.

Or, de tels traitements requièrent une protection spécifique³⁴² 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.

Ainsi, lors de la mise en œuvre des traitements de données dites sensibles, le responsable du traitement devra particulièrement veiller au respect des dispositions de l'article 9, paragraphe (2) du RGPD.

B. Quant aux données à caractère personnel visées par les dispositions du chapitre 2 du projet de loi

1. Ad article 6 du projet de loi

L'article 6 du projet de loi traite des différentes informations que l'établissement hospitalier ou tout autre professionnel ayant encadré la naissance sont amenés à collecter et à transmettre au ministre.

i. L'insécurité juridique liée à l'imprécision des termes employés

Les termes employés à l'article 6 sont vagues de sorte qu'il est difficile de savoir quelles informations seraient susceptibles d'être collectées et transmises au ministre et, le cas échéant, à l'enfant.

En effet, il ressort dudit article que les parents de naissance sont invités à laisser des « *informations médicales sur [leur] santé, et celle de*

³⁴² 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.

l'autre parent de naissance, des informations sur les origines de l'enfant, les circonstances de l'enfant de la naissance ainsi que toute autre information qu'[ils] souhaite[nt] mettre à disposition de [leur] enfant»³⁴³.

Les auteurs du projet de loi dans le commentaire des articles précisent à ce sujet que les parents de naissance sont invités à laisser « *toute sorte d'informations* » et que les informations précitées constituent des « *informations non-identifiantes* »³⁴⁴.

Les auteurs du projet de loi ne fournissent dès lors pas d'explications sur ce qu'il faut entendre par « *informations non-identifiantes* ».

Il convient toutefois de souligner que le RGPD aura vocation à s'appliquer à toute information se rapportant à une personne physique identifiée ou identifiable³⁴⁵. Le considérant 26 du RGPD précise que « *[p]our déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement [...]* ».

Ainsi, la CNPD donne à considérer que le cumul d'informations, même qualifiées de « *non-identifiantes* », comporte le risque d'une (ré)identification de la personne physique en question, ayant pour conséquence l'application des règles relatives à la protection des données.

L'article 6, paragraphe 3, du projet de loi prévoit encore l'obligation pour l'établissement hospitalier ainsi que tout autre professionnel ayant encadré la naissance de collecter des « *informations non-identifiantes* ». Les auteurs du projet de loi n'apportent là encore dans leur commentaire des articles aucune précision quant aux informations qui seraient collectées.

Par ailleurs, il y a lieu de relever que l'article 12 du projet de loi utilise par la suite les termes « *renseignements ne portant pas atteinte à l'identité d'un ou des parents de naissance* ». La CNPD suppose qu'il s'agit des « *informations non-identifiantes* » visées à l'article 6. Afin d'éviter toute confusion, il est suggéré d'utiliser la même terminologie à travers l'intégralité du projet de loi.

Enfin, il y a encore lieu de constater que faculté est laissée aux parents de naissance de faire une déclaration de son identité³⁴⁶, auquel cas ces informations sont à considérer comme des données à caractère personnel.

La CNPD suppose que les auteurs du projet de loi sous avis se sont inspirés de la loi française du 2 août 2021 relative à la bioéthique qui prévoit que dans le cadre d'une PMA les tiers donneurs doivent fournir non seulement leur identité, mais également des données « *non identifiantes* ». En effet, l'article 5 de ladite loi française insère un chapitre dans le code de la santé publique sur l'« *Accès aux données non identifiantes et à l'identité du tiers donneurs* ». Dans ce chapitre figure notamment l'article L. 2143-3. qui comporte une liste de don-

³⁴³ Article 6, paragraphe 1, point 2° et paragraphe 2, point 1° du projet de loi.

³⁴⁴ Commentaire des articles, article 6 page 17.

³⁴⁵ Article 4, point 1) du RGPD.

³⁴⁶ Article 6, paragraphe (1), points 2° et 3°, et paragraphe (2), points 2° et 3° du projet de loi.

6

ANNEXES

nées non identifiantes des tiers donneurs, à savoir : leur âge, leur état général tel qu'ils le décrivent au moment du don, leur caractéristique physiques, leur situation familiale et professionnelle, leur pays de naissance ainsi que les motivations de leur don, rédigées par leurs soins.

Par conséquent, au regard de l'imprécision des termes utilisés par les auteurs du projet de loi et du flou juridique y résultant, il convient de constater 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'homme³⁴⁷.

Afin de parer à cette insécurité juridique quant aux catégories de données qui seraient traitées 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 préciser, à l'instar de la loi française relative à la bioéthique du 2 août 2021, quelles catégories de données seraient susceptibles d'être traitées par le ministre.

En tout état de cause, l'imprécision des termes employés complique, voire rend impossible, la tâche de la Commission nationale d'apprécier si le projet de loi respecte le principe de minimisation des données consacré à l'article 5, paragraphe 1^{er}, lettre c) du RGPD selon lequel 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.

Le caractère nécessaire s'apprécie par rapport à la finalité du traitement telle que définie par les auteurs du projet de loi, à savoir « *la mise en œuvre de la recherche de l'accès d'un enfant à ses origines [...]* »³⁴⁸. Or, tel que mentionné au point II.B. les imprécisions quant aux finalités recherchées, ne permettent pas de déterminer dans quelle mesure le traitement de ces données est nécessaire pour exercer le droit de connaître ses origines.

ii. Le traitement des données concernant la santé

L'article 6, paragraphes 1er et 2 du projet de loi prévoit la possibilité pour le parent qui a accouché l'enfant de laisser des « *informations médicales sur sa santé et celle de l'autre parent de naissance* » ou respectivement pour l'autre parent de naissance de laisser des « *informations médicales sur sa santé et celle du parent qui a accouché l'enfant* ».

De plus, l'article 6, paragraphe 3, du projet de loi crée l'obligation pour l'établissement hospitalier ainsi que pour tout autre professionnel ayant encadré la naissance de « *recueillir dans la mesure du possible [...] des données médicales d'un ou des deux parents de naissance lors de la naissance et de les transmettre au ministre* ».

Ces informations relatives à la santé des parents de naissance, et si celles-ci constituent

³⁴⁷ 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, CourEDH, Vavříčka et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.

³⁴⁸ Article 4, paragraphe 3, du projet de loi

des données à caractère personnel, constituent des données dites sensibles. Le traitement de telles données doit dès lors reposer sur une des conditions visées à l'article 9, paragraphe 2 du RGPD. Sur ce point, il est renvoyé au point A du point IV du présent avis.

Par ailleurs, il y a lieu de regretter que ni l'exposé des motifs ni le commentaire des articles ne fournissent des explications quant aux modalités des traitements de « données médicales ».

Dans ce contexte, la Commission nationale se rallie aux préoccupations soulevées par le Conseil d'Etat quant à l'article 6 du projet de loi et notamment en ce qu'il considère que « [s]i les parents ne sont pas invités à révéler l'identité de l'autre parent, ils peuvent néanmoins laisser des informations médicales sur l'autre parent. Or, il revient à chaque parent de décider s'il veut communiquer les informations médicales sur sa santé. Comment articuler le choix laissé au parent de ne pas communiquer ses données médicales avec la possibilité pour l'autre parent de les fournir à son insu ? Si le législateur permet à chacun des parents de ne pas communiquer les informations sur sa santé ou sur son identité, il est difficile de voir comment articuler le respect de ces secrets respectifs »³⁴⁹.

Dans ce contexte, la Commission nationale se pose la question de savoir comment le responsable du traitement entend respecter le principe d'exactitude, prévu à l'article 5, paragraphe 1^{er}, lettre d) du RGPD. La Commission nationale

renvoie à cet égard à ses développements sur le respect du principe d'exactitude au point VIII du présent avis.

Il convient également de soulever que l'imprécision des termes « *dans la mesure du possible* » repris à l'article 6, paragraphe 3, du projet de loi résulte en un flou juridique, de manière à constater 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'homme³⁵⁰.

En outre, il convient encore de s'interroger sur l'articulation entre l'obligation pour l'établissement hospitalier, ainsi que pour tout autre professionnel ayant encadré la naissance, prévue par l'article 6, paragraphe 3, du projet de loi, et le secret médical auquel sont soumis ces personnes.

2. Ad article 10 du projet de loi

L'article 10, point 5^o, du projet de loi prévoit que le ministre est amené à recevoir « [I] es déclarations d'identité formulées par les ascendants, descendants et collatéraux des parents de naissance ».

Toutefois, le projet de loi ne fournit pas d'autres précisions ou explications quant aux catégories de données à caractère personnel qui figure-raient sur lesdites « déclarations d'identité ».

En outre, il y a lieu de s'interroger sur la manière dont ces données seraient collectées :

³⁴⁹ Avis n°60.376 du 16 juillet 2021 du Conseil d'Etat sur le projet de loi portant organisation de l'accès à la connaissance de ses origines dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs, p.6 à 8

³⁵⁰ 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, CourEDH, Vavříčka et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.

6

ANNEXES

appartient-il aux ascendants, descendants et collatéraux de s'adresser directement au ministre ? Comment le ministre assurera-t-il que les déclarations d'identité sont attribuées à l'enfant concerné, étant donné que seuls les prénoms et le sexe de l'enfant ainsi que la date et le lieu de naissance (et non pas l'identité des parents de naissance) sont mentionnés à l'extérieur des plis visés à l'article 6 du projet de loi ? Le ministre vérifiera-t-il s'il existe effectivement un lien de parenté entre ces personnes et les parents de naissance ?

En vertu des articles 13 et 14 du projet de loi, le ministre communique, ensemble avec l'identité du parent qui a accouché l'enfant ou de l'autre parent de naissance, les informations visées au point 5 de l'article 10. Est-ce que cela veut dire que les déclarations d'identité des ascendants, descendants et collatéraux du parent qui a accouché l'enfant sont communiquées à l'enfant, même si seul l'autre parent de naissance a accordé la levée du secret de son identité, et vice versa ? Une telle façon de procéder contrecarrerait pourtant leur volonté de rester anonyme et porterait atteinte à l'intimité de leur vie privée. La Commission nationale estime que les auteurs du projet de loi devraient préciser les modalités pratiques applicables aux déclarations d'identité formulées par les ascendants, descendants et collatéraux des parents de naissance.

3. Ad article 16 du projet de loi

Pour les demandes d'accès aux origines formulées par des enfants ayant fait l'objet

d'une adoption nationale mais ne tombant pas sous le régime de l'accouchement sous secret, il résulte de l'article 16 du projet de loi que le ministre « *recueille les informations relatives à l'identité du parent qui a accouché l'enfant et de l'autre parent de naissance auprès des autorités judiciaires* ».

Or, ni le commentaire des articles, ni l'exposé des motifs ne précisent ce qu'il faut entendre par « informations relatives à l'identité ». S'agit-il seulement du nom et prénom ou cette notion vise-t-elle également d'autres données, comme par exemple l'adresse ?

De plus, le projet de loi ne précise pas les modalités selon lesquelles le ministre obtiendrait de telles « informations ».

Des précisions devraient être apportées à ce sujet à l'article 16 du projet de loi afin de clarifier quelles données seraient collectées et de quelle manière le ministre les collecterait.

4. Ad article 17 du projet de loi

L'article 17 du projet de loi entend régler la gestion des demandes d'accès aux origines formulées par des enfants ayant fait l'objet d'une adoption internationale.

En vertu des dispositions de l'article précité, le ministre peut obtenir « *sur demande* » de la part des organismes visés audit article « *toutes les informations relatives aux origines de l'adopté* ».

Or, cette formulation est particulièrement vague et nécessite des clarifications. En effet, il y a lieu de se demander ce que les auteurs du projet de loi ont voulu entendre par « les informations relatives aux origines de l'adopté ». Quelles informations seraient visées concrètement ?

Le ministre peut encore obtenir « auprès des autorités du pays d'origine de l'enfant toutes les informations qu'il peut obtenir sur les origines de l'enfant ». Cette formulation est également particulièrement vague. Quelles informations le ministre pourrait-il recueillir auprès des autorités étrangères ?

A ce titre, il convient de relever que la Convention de la Haye du 29 mai 1993 sur la protection des enfants et la coopération en matière d'adoption internationale dispose d'ores et déjà dans son article 16, paragraphe 1^{er}, lettre a) que :

« Si l'Autorité centrale de l'Etat d'origine considère que l'enfant est adoptable, a) elle établit un rapport contenant des renseignements sur l'identité de l'enfant, son adoptabilité, son milieu social, son évolution personnelle et familiale, son passé médical et celui de sa famille, ainsi que sur ses besoins particuliers ; (...) ».

En outre, la Convention de la Haye du 29 mai 1993 sur la protection des enfants et la coopération en matière d'adoption internationale prévoit encore explicitement à l'article 16, paragraphe 2 que l'Autorité centrale de l'Etat d'origine « transmet à l'Autorité centrale de l'Etat d'accueil son rapport sur l'enfant, la preuve

des consentements requis et les motifs de son constat sur le placement, en veillant à ne pas révéler l'identité de la mère et du père, si, dans l'Etat d'origine, cette identité ne peut pas être divulguée ».

Dès lors, la Commission nationale se demande quelles informations supplémentaires pourraient, le cas échéant, être recueillies alors que les dispositions précitées prévoient qu'un rapport sur l'enfant sera transmis à l'Autorité centrale de l'Etat d'accueil.

C. Quant aux données à caractère personnel visées par le chapitre 3 du projet de loi

L'article 20 consacre l'obligation des auteurs du projet parental à fournir au responsable du traitement, c'est-à-dire au ministre, les informations énumérées aux points 1^o à 4^o dudit article.

S'il y a lieu de saluer l'inclusion d'une liste déterminée d'informations à fournir au ministre, il convient de s'interroger sur les informations qui seraient visées au dernier alinéa du paragraphe 1^{er} de l'article 20 qui dispose que « toute autre information disponible sur le ou les tiers donneurs peut également être communiquée ».

En effet, la notion de « toute information » est très vague et le commentaire des articles n'apporte pas de précision à cet égard.

Or, il y a lieu de rappeler qu'en vertu du principe de minimisation des données, consacré

6

ANNEXES

à l'article 5, paragraphe 1, lettre c) du RGPD, les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

En l'absence de telles précisions, la CNPD n'est pas en mesure d'apprécier si un tel principe serait respecté et estime partant nécessaire que le projet de loi détermine précisément quelles données à caractère personnel seraient susceptibles d'être déclarées au ministre.

Dans l'état actuel du projet de loi, les auteurs du projet parental pourraient estimer opportun de transmettre au ministre des données dites sensibles, tel que par exemple des données concernant la santé du ou des tiers donneurs, qui sont pourtant soumises à un régime plus strict. La Commission nationale renvoie à cet égard à ses développements au point IV.A. du présent avis.

Par ailleurs, il convient de noter que l'obligation de fournir ces informations incombe, conformément à l'article 20, paragraphe 1^{er} du projet de loi sous avis, aux parents du projet parental. La CNPD note que l'article 19 du projet de loi prévoit encore que *« le centre de fécondation, tout médecin chargé de mettre en œuvre la procréation médicalement assistée ainsi que les auteurs du projet parental ont l'obligation de vérifier si les informations énumérées à l'article 20, point 4 se trouvent dans le dossier avant l'insémination des gamètes ou de l'implantation des embryons surnuméraires »*. Elle note encore que parmi

les informations à fournir figurent aux point 4^o du 1^{er} paragraphe de l'article 20 *« l'identité du ou des tiers donneurs y compris nom, prénom, date et lieu de naissance, nationalité(s), adresse actuelle, état civil ainsi que le numéro de matricule s'il existe »*.

Or, la Commission nationale s'interroge sur la source initiale de ces informations. Est-ce qu'il appartient au centre de fécondation, au médecin chargé de mettre en œuvre la procréation médicalement assistée, aux auteurs du projet parental ou à un autre intervenant encore d'inscrire cette information dans le dossier visé à l'article 19 ?

La question se pose notamment dans le contexte de l'obligation du responsable du traitement d'informer la personne concernée. En effet, la Commission nationale comprend que dans le cadre d'une PMA, la collecte des données à caractère personnel du tiers donneur par les acteurs impliqués, à savoir le responsable du traitement, les auteurs du projet parental, le centre de fécondation ou encore tout médecin chargé de mettre en œuvre la procréation médicalement assistée, est opérée de manière indirecte, donc les informations ne sont pas collectées directement auprès de la personne concernée. Or, l'article 14 du RGPD oblige le responsable du traitement à fournir certaines informations à la personne concernée lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée. L'article 14, paragraphe 2, lettre f), du RGPD exige notamment que le responsable du traitement informe sur *« la source d'où*

proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public ». La Commission nationale se demande à qui incomberait cette obligation, voire toute autre obligation découlant du RGPD, si, tel que mentionné au point II du présent avis, les rôles (responsable du traitement, responsable du traitement conjoint ou sous-traitant) des différents intervenants n'est pas clair.

En l'absence de précisions, la CNPD se voit dans l'impossibilité de vérifier si les exigences du RGPD envers la personne concernée seraient respectées par le projet de loi sous avis.

D. Quant aux données à caractère personnel visées par les dispositions du chapitre 5 du projet de loi

1. Ad article 25 du projet de loi

Il ressort du commentaire des articles que l'article 25 du projet de loi vise les enfants nés avant l'entrée en vigueur de la future loi dans le cadre d'un accouchement sous secret.

Le paragraphe 2, alinéa 1^{er}, de l'article 25 dispose que « *[I]es établissements hospitaliers, les autres professionnels ayant encadré la naissance de l'enfant [...], ainsi que les organismes autorisés et habilités pour l'adoption conformément à la loi du 31 janvier 1998 portant agrément des services d'adoption et définition des obligations leur incombant ainsi que tout autre organisme ou autorité nationale intervenus dans le cadre de l'adoption ont l'obligation de*

communiquer des éléments relatifs à l'identité des parents de naissance ou toute autre information, dossier et objet matériel laissé par le ou les parents de naissance au ministre dans les cas visés au paragraphe précédent dans un pli fermé ».

Selon le commentaire des articles, cette disposition constitue la base légale pour ces différents intervenants de « *transférer tous les dossiers qu'ils détiennent au Ministre* » sans toutefois préciser quelles seraient les données à caractère personnel qui seraient collectées à cette occasion.

S'il y a lieu de saluer les auteurs du projet de loi de créer une base légale permettant aux intervenants précités de communiquer au ministre les informations qu'ils ont pu recueillir avant l'entrée en vigueur de la loi, en l'absence de précisions quant aux catégories de données à caractère personnel qui seraient communiquées dans ce contexte, la Commission nationale n'est pas en mesure d'apprécier si le principe de minimisation des données serait en l'espèce respecté.

Il convient de rappeler qu'en vertu du principe de minimisation, 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.

Conformément à ce principe, les différents intervenants précités devraient dès lors s'assurer à ne transmettre au ministre que les données à caractère personnel adéquates,

6

ANNEXES

pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Enfin, dans la mesure où les termes suivants « *ont l'obligation de communiquer des éléments relatifs à l'identité des parents de naissance ou toute autre information, dossier et objet matériel laissé par le ou les parents de naissance au ministre* » sont formulés de manière vague, et que le commentaire des articles n'apporte pas de précision à cet égard, la Commission nationale estime partant nécessaire que le projet de loi détermine précisément quelles données à caractère personnel seraient susceptibles d'être communiquées au ministre.

2. Ad article 26 du projet de loi

En vertu de l'article 26 du projet de loi, visant les autres adoptions nationales ainsi que les adoptions internationales, les organismes y mentionnés ont l'obligation de communiquer « *des éléments relatifs à l'identité des parents de naissance ou toute autre information, dossier et objet matériel laissé par le ou les parents de naissance au ministre [...] dans un pli fermé* » et que « *les prénoms donnés à l'enfant et, le cas échéant, mention du fait qu'ils l'ont été par la mère de naissance ou l'autre parent de naissance au ministre compétent ainsi que le sexe de l'enfant et la date, le lieu et l'heure de sa naissance sont mentionnés à l'extérieur de ces plis* ».

S'il y a lieu de féliciter les auteurs du projet de loi pour avoir précisé les données qui seraient

communiquées au ministre, il y a lieu de regretter que les termes « *toute autre information, dossier* » sont trop vagues de sorte que la CNPD n'est pas en mesure d'apprécier si le principe de minimisation serait respecté.

Les auteurs du projet de loi devraient apporter des précisions à cet égard.

Par ailleurs, il y a lieu de relever qu'une telle obligation n'existe pas sous les articles 16 et 17 du projet de loi, dès lors ne serait-il pas opportun d'aligner cette disposition transitoire sur ce qui est prévu dans ces articles ?

V. Sur l'accès au RNPP et aux registres de l'état civil

En vertu de l'article 5, paragraphe 1^{er}, lettre c) du RGPD, 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.

L'article 4, paragraphe 6 du projet de loi prévoit la possibilité pour le ministre de consulter le registre national des personnes physiques (ci-après le « *RNPP* ») ainsi que les registres de l'état civil.

La disposition se limite à indiquer que le responsable du traitement dispose de cet accès « *dans le cadre de la finalité déterminée au paragraphe 3* ». Ni le commentaire des articles, ni l'exposé des motifs n'apportent de précisions quant aux raisons qui justifieraient un tel accès.

Or, il y a lieu de s'interroger sur l'articulation de ces dispositions avec celles relatives à l'article 9 du projet de loi qui prévoient qu'aucune enquête ne serait effectuée concernant les informations fournies par le parent qui a accouché l'enfant ou l'autre parent de naissance.

Ainsi, il y a lieu de se demander si la consultation du RNPP et des registres d'état civil permettrait au responsable du traitement de vérifier la réalité du lien de parenté entre ces personnes et les parents de naissance ? Dans un souci de sécurité juridique, des précisions devraient être apportées au projet de loi à ce sujet.

La CNPD n'est dès lors pas en mesure d'apprécier si la consultation du RNPP et des registres de l'état civil respecte le principe de minimisation des données prévu à l'article 5, paragraphe 1er, lettre c) du RGPD.

VI. Sur l'accès aux archives de la juridiction tel que visé à l'article 25 du projet de loi

L'article 25, paragraphe 3 du projet de loi prévoit que le ministre « *peut consulter les archives de la juridiction ayant prononcé l'adoption ainsi que les dossiers de protection internationale auprès du Ministre ayant la protection internationale dans son ressort* ».

La Commission nationale se demande ce que le verbe « *consulter* » veut dire. S'agit-il d'une demande d'accès que le ministre introduit auprès du ministre ayant la protection

internationale dans son ressort ? Ou s'agit-il d'un accès direct ? La Commission nationale se demande encore si les données issues de cette consultation seront intégrées dans le fichier centralisé géré par le ministre.

Par ailleurs, il convient de se rallier aux observations du Conseil d'Etat quant à la finalité d'une telle consultation qui devrait être ajoutée aux finalités mentionnées à l'article 4, paragraphe 3, du projet de loi sous avis³⁵¹.

VII. Sur la sécurité du traitement

Il convient encore de rappeler que les règles applicables en matière de protection des données s'appliquent indépendamment des techniques utilisées, c'est-à-dire tant aux données appelées à être contenues dans un fichier papier qu'un fichier informatique.

Ce rappel paraît nécessaire vu que, pour les adoptions suite à des accouchements sous secret par exemple, les informations fournies, dont des données à caractère personnel, semblent être rédigées sur papier dans un pli fermé. Les plis sont ensuite transmis au ministre.

En ce qui concerne la sécurité du traitement, le point 4 du paragraphe 5 de l'article 4 du projet de loi indique que le responsable du traitement doit mettre en place des mesures techniques et organisationnelles afin d'assurer la sécurité et la confidentialité des données à caractère personnel, sans toutefois donner de précision quelconque.

³⁵¹ Avis n°60.376 du 16 juillet 2021 du Conseil d'Etat sur le projet de loi portant organisation de l'accès à la connaissance de ses origines dans le cadre d'une adoption ou d'une procréation médicalement assistée avec tiers donneurs, p.5.

6

ANNEXES

Or, cette obligation générale de sécurité relève tant de l'article 5, paragraphe 1^{er}, lettre f) du RGPD qui consacre le principe d'intégrité et confidentialité que de l'article 32 du RGPD qui précise davantage la notion de sécurité des données dans le cadre de la protection des données à caractère personnel.

En l'espèce, l'obligation du responsable de traitement de garantir un niveau de sécurité adapté aux risques pour les droits et libertés des personnes physiques concernées par les traitements de données personnelles envisagés, mérite une attention particulière dans la mesure où des accès non-autorisés aux données, des fuites de données ou encore des modifications non-désirées sont susceptibles de causer un préjudice grave aux personnes concernées.

Ainsi, eu égard à la nature des données traitées en cause, il est essentiel que de telles mesures de sécurité soient mises en œuvre par le responsable du traitement afin d'assurer la confidentialité et la sécurité des données. 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.

Dans l'hypothèse où un outil informatique serait utilisé pour traiter les données en cause, ce qui semble être le cas au vu de la fiche financière du projet de loi, il serait nécessaire de prévoir un système de journalisation des accès. Sur ce point, la CNPD recommande que

les données de journalisation soient conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.

La CNPD souligne aussi l'importance d'effectuer pro-activement des contrôles en interne. A cet effet, il convient conformément à l'article 32, paragraphe 1, lettre d) du RGPD de mettre en œuvre une procédure « *visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».

En outre, la Commission nationale estime essentiel, au regard de la sensibilité de certaines données traitées, de prévoir les modalités de mise en œuvre de ce principe d'intégrité et de confidentialité dans un texte d'ordre législatif ou du moins d'ordre réglementaire.

VIII. Les droits des personnes concernées

Comme les parents de naissance sont susceptibles d'être qualifiés de personnes concernées au sens du RGPD pour les traitements de données qui résultent du projet de loi, il convient de rappeler que l'article 5, paragraphe 1^{er}, lettre a) ainsi que les articles 12, 13 et 14 du RGPD exigent du responsable du traitement d'agir en toute transparence à l'égard des personnes concernées en leur fournissant notamment certaines informations sur les traitements de données à caractère personnel envisagés.

Dans l'hypothèse où le ministre collecterait indirectement des données à caractère personnel, tel que cela semble résulter notamment de l'article 5, 16 ou encore 17 du projet de loi, le ministre devra respecter les dispositions de l'article 14 du RGPD.

Dans ce contexte, il convient d'attirer l'attention des auteurs du projet de loi sur l'article 14, paragraphe 4, du RGPD en vertu duquel « *[I] orsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2* ».

Le paragraphe 5 de cet article énumère les hypothèses dans lesquelles les paragraphes 1 à 4 ne s'appliquent pas. Si les auteurs du projet de loi entendent invoquer l'article 14, paragraphe 5, lettre c) du RGPD pour justifier, le cas échéant, le fait de ne pas fournir les informations mentionnées aux paragraphes 1 à 4, il y a lieu de souligner qu'une telle dispense ne peut s'appliquer que si le droit national « *prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée* ».

En ce qui concerne les données à caractère personnel relatives au tiers donneur qui seraient collectées en application de l'article 20, paragraphe 4 du projet de loi, il convient

d'attirer l'attention des auteurs du projet de loi sur le fait que ce dernier dispose d'un droit à l'information en vertu de l'article 14 du RGPD ou encore d'un droit de rectification, qui lui est conféré par l'article 16 du RGPD. Il devrait dès lors pouvoir s'adresser au responsable du traitement pour demander la rectification des données qui ne seraient éventuellement plus à jour ou inexactes.

De plus, l'article 6 du projet de loi prévoit que le parent qui a accouché l'enfant peut transmettre des informations concernant l'autre parent de naissance, et vice versa. L'article 14 du RGPD aurait dès lors vocation à s'appliquer dans la mesure où cette disposition précise les informations à fournir par le responsable du traitement lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée elle-même.

De manière générale, et compte tenu de l'objet du projet de loi, la Commission nationale se demande comment les droits de personnes concernées s'articuleraient avec certaines des dispositions du projet de sous avis.

En effet, en plus du droit à l'information susmentionné, le RGPD confère d'autres droits aux personnes concernées que le responsable du traitement est tenu de respecter, notamment le droit d'accès et le droit de rectification prévus respectivement à l'article 15 et l'article 16 du RGPD. Dans le cadre du projet de loi sous avis, se pose en particulier la question de savoir comment le responsable du traitement entend mettre œuvre en pratique les exigences

6

ANNEXES

qui découlent pour lui de ces droits. Comment le responsable du traitement entend-il communiquer aux personnes concernées les informations nécessaires dans le contexte du droit à l'information, notamment s'il collecte les données à caractère personnel de façon indirecte ? Comment les personnes concernées peuvent-elles exercer leurs droits ? Dans l'hypothèse d'un accouchement sous secret pour lequel aucune déclaration d'identité n'a été reçue, mais pour lequel les établissements hospitaliers communiquent des données « non-identifiantes », comment le responsable du traitement entend-il donner suite à une demande de droit d'accès ?

Par ailleurs, se posent également des interrogations sur le respect, par le responsable du traitement, des principes relatifs au traitement des données à caractère personnel consacrés à l'article 5 du RGPD. Ainsi, le responsable du traitement doit par exemple, s'assurer qu'il traite les données à caractère personnel de manière licite, loyale et transparente au regard de la personne concernée (principe de licéité, loyauté et transparence) et uniquement des données exactes et, si nécessaire, tenues à jour (principe d'exactitude). Ainsi, comment le responsable du traitement entend-il s'assurer qu'il ne traite pas des données à caractère personnel d'une personne concernée à l'insu de cette dernière ? Comment le responsable du traitement peut-il s'assurer de l'exactitude des données, notamment si les données sont collectées de manière indirecte ? De même, comment peut-il s'assurer de l'exactitude des données d'identité fournies directement si, dans l'hypothèse d'un

accouchement sous secret, aucune vérification (article 9 du projet de loi sous avis) n'est prévue ?

Ainsi, si les auteurs du projet de loi entendent limiter la portée des droits des personnes concernées, voire des obligations incombant au responsable du traitement, en ayant recours à la possibilité fournie par l'article 23 du RGPD une telle limitation devrait être prévue par une mesure législative et répondre aux critères et exigences énumérés audit article.

IX. Sur la durée de conservation

Selon le principe de limitation de la conservation consacré à l'article 5, paragraphe 1^{er}, 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. Au-delà, les données doivent être supprimées ou définitivement anonymisées.

S'il y a lieu de féliciter les auteurs du projet de loi de prévoir à l'article 4, paragraphe 2 du projet de loi un délai de conservation des données, à savoir pendant 100 ans et que les données seraient détruites après l'écoulement de cette période, la Commission nationale se trouve dans l'impossibilité d'apprécier si, en l'occurrence, le principe de la limitation de la conservation est respecté.

En effet, ni le commentaire des articles, ni l'exposé des motifs ne fournissent des explications quant aux critères ayant servi à la détermination de cette période de conservation des données.

Il y a lieu de constater que conformément à l'article 11, alinéa 3, point 5 du projet de loi, la demande d'accès à la connaissance des origines peut être introduite par les descendants en ligne directe majeurs de l'enfant jusqu'au 1^{er} degré, s'il est décédé. Dès lors la durée de conservation de 100 ans viserait-elle à permettre aux descendants directs au premier degré d'exercer leur droit d'accès aux origines ?

Il convient encore de noter que le projet de loi ne prévoit pas la suppression des données personnelles une fois que l'enfant aurait exercé son droit d'accès aux origines. Elle suppose que les données sont conservées pour permettre, le cas échéant, aux descendants directs au premier degré d'exercer à leur tour ce droit.

Or, faute d'explications quant aux critères ayant servi à la détermination de cette période de conservation des données par les auteurs du projet de loi, la CNPD ne peut pas se prononcer sur la proportionnalité du délai retenu. De telles précisions devraient dès lors être apportées par les auteurs du projet de loi.

X. L'analyse d'impact relative à la protection des données

L'article 35, paragraphe 10, du RGPD, lu ensemble avec l'article 36, paragraphes 1^{er} et 4, du RGPD indiquent qu'en cours d'élaboration d'une mesure législative devant être adoptée par un parlement national, les auteurs de cette mesure législative peuvent être amenés à réaliser une analyse d'impact sur la protection des données (ci-après « l'AIPD »), et que le

résultat de l'AIPD pourrait conduire à une consultation préalable de l'autorité nationale compétente, en l'occurrence la CNPD.

Etant donné qu'il ressort de l'article 35, paragraphe 1^{er}, du RGPD qu'une AIPD devrait être réalisée si le traitement envisagé est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques compte tenu de la nature, de la portée, du contexte et des finalités du traitement, la Commission nationale se demande si les traitements envisagés par le projet de loi sous avis n'auraient pas dû faire l'objet d'une AIPD par les auteurs. Le cas échéant, l'AIPD aurait indiqué que le traitement présente un risque élevé conduisant ainsi les auteurs du projet de loi, éventuellement déjà au stade de l'élaboration de l'avant-projet de loi, à consulter la CNPD.

Ainsi décidé à Belvaux en date du 29 novembre 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7924 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19. (Délibération n° 53/AV31/2021 du 8/10/2021)

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 courriel en date du 4 décembre 2021, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur le projet de loi n° 7924 portant modification de la

loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19³⁵² (ci-après le « projet de loi n° 7924 »).

D'après l'exposé des motifs, en raison de la situation épidémiologique très préoccupante et de l'évolution du contexte sanitaire sur plusieurs fronts, le projet de loi n° 7924 « *se propose d'apporter des modifications substantielles à la version actuelle de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 qui vient, en principe, à échéance le 18 décembre 2021. Pour des raisons de santé et de sécurité des citoyens, il est d'ailleurs proposé de ne pas attendre cette échéance pour mettre en place les nouvelles mesures.* »

La CNPD constate dans ce contexte que les articles 5 et 10 de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 (ci-après : « loi modifiée du 17 juillet 2020 ») concernant notamment le traçage des contacts et le traitement de données à caractère personnel par la Direction de la santé à travers la mise en place d'un système d'information, n'ont pas subi de modifications.

Néanmoins, elle souhaite s'exprimer sur deux nouveautés intégrées dans le projet de loi sous avis impliquant des questions relatives à la pro-

³⁵² Intitulé entier : « *Projet de loi n° 7924 portant modification: 1° de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 ; 2° de la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments ; 3° de la loi modifiée du 6 janvier 1995 relative à la distribution en gros des médicaments ; 4° de la loi modifiée du 24 juin 2020 portant introduction de mesures temporaires relatives à la loi communale modifiée du 13 décembre 1988 et à la loi modifiée du 27 mars 2018 portant organisation de la sécurité civile dans le cadre de la lutte contre le Covid-19 ; 5° de la loi modifiée du 24 juin 2020 portant introduction d'une mesure temporaire relative à l'application de l'article 12 de la loi modifiée du 19 juillet 2004 concernant l'aménagement communal et le développement urbain dans le cadre de la lutte contre le Covid-19 ; 6° de la loi modifiée du 24 juin 2020 concernant la célébration du mariage dans un édifice communal autre que la maison communale dans le cadre de la lutte contre la pandémie Covid-19 ; 7° de la loi du 24 juillet 2020 portant dérogation temporaire aux articles L. 524-1, L. 524-2, L. 524-5, L. 541-1 et L. 541-2 du Code du travail ; 8° de la loi modifiée du 20 juin 2020 portant 1° dérogation temporaire à certaines dispositions en matière de droit du travail en relation avec l'état de crise lié au Covid-19 ; 2° modification du Code du travail ; 9° de la loi modifiée du 19 décembre 2020 portant dérogation temporaire à l'article L. 121-6 du Code du travail ; 10° de la loi modifiée du 19 décembre 2020 ayant pour objet la mise en place d'une contribution temporaire de l'Etat aux coûts non couverts de certaines entreprises ; 11° de loi modifiée du 19 décembre 2020 ayant pour objet la mise en place d'une nouvelle aide de relance ; 12° de la loi modifiée du 22 janvier 2021 portant : 1° modification des articles L. 234-51, L. 234-52 et L. 234-53 du Code du travail ; 2° dérogation temporaire aux dispositions des articles L. 234-5, L. 234-52 et L. 234-53 du Code du travail.* »

tection des données, et plus spécifiquement sur l'obligation pour les exploitants d'établissements ou les organisateurs de rassemblements, de manifestations ou d'événements (ci-après : « les exploitants et organisateurs ») sous régime Covid check de demander une pièce d'identité à la personne qui leur présente un certificat de vaccination ou de rétablissement, d'une part (1), ainsi que sur la possibilité de tenir une liste des personnes vaccinées dans le cadre du Covid check par lesdits exploitants ou organisateurs, d'autre part (2).

Quant à l'obligation de présenter une pièce d'identité dans le cadre du régime Covid check

Le nouveau point 27, alinéas 2 et 3 de l'article 1^{er} de la loi modifiée du 17 juillet 2020 entend modifier la définition du « régime Covid check » en prévoyant, entre autres, que « *l'exploitant de l'établissement ou l'organisateur du rassemblement, de la manifestation ou de l'évènement sous régime Covid check est tenu de demander une pièce d'identité à la personne qui lui présente un certificat de vaccination ou de rétablissement afin de s'assurer que l'identité mentionnée sur le certificat présenté et celle figurant sur la pièce d'identité sont identiques.* »

La CNPD comprend du libellé de l'article cité que les exploitants et organisateurs n'ont pas seulement la faculté, mais par contre une obligation de demander systématiquement une pièce d'identité à la personne qui lui présente un certificat de vaccination ou de rétablissement afin d'éviter tout risque d'abus.

Les auteurs du projet de loi n° 7924 utilisent le terme « pièce d'identité », mais ne le définissent pas, de sorte qu'il faut partir du principe que les personnes concernées ne doivent pas forcément montrer leur carte d'identité, mais que tout autre document d'identité est susceptible de servir comme pièce d'identité, à savoir passeport, permis de conduire ou autres. Or, sans définir le terme pièce d'identité, il n'est pas aisé d'apprécier l'étendue dudit terme et posera des problèmes en pratique pour ceux qui sont obligés de mettre en œuvre cette disposition légale.

Par ailleurs, il y a lieu de rappeler que le RGPD n'a vocation à s'appliquer que lorsqu'un traitement de données à caractère personnel³⁵³ est effectué. Le simple fait que les exploitants et organisateurs visionnent les données à caractère personnel figurant sur une pièce d'identité ne constitue pas un traitement de données au sens du RGPD. Il en irait autrement si les exploitants et organisateurs étaient amenés à créer un fichier reprenant l'ensemble des données figurant sur les pièces d'identité des personnes contrôlées ou contenant des copies des pièces d'identité. En effet, en l'état actuel du droit, et sauf si un texte légal en prévoit expressément la possibilité, il s'agirait alors d'un traitement de données disproportionné, qui ne respecterait pas le principe de minimisation des données, dans la mesure où des moyens moins attentatoires à la vie privée des personnes concernées pourraient être mis en œuvre afin d'atteindre la finalité prévue, c'est-à-dire s'assurer par un contrôle visuel de ladite pièce que l'identité mentionnée sur le

³⁵³ Voir la définition du traitement de données prévu à l'article 4.2 du RGPD, ainsi que son champ d'application matériel prévu à l'article 2.1 du RGPD.

6

ANNEXES

certificat présenté correspondre bien à celle figurant sur la pièce d'identité.

Quant à la possibilité de tenir une liste des personnes vaccinées

Le nouveau point 27, alinéa 4 de l'article 1^{er} de la loi modifiée du 17 juillet 2020 prévoit par ailleurs que pour « *faciliter les vérifications effectuées dans le cadre du Covid check, tout exploitant ou organisateur peut tenir une liste des personnes vaccinées lorsque celles-ci accèdent régulièrement à un établissement donné ou participent régulièrement à des activités ou événements soumis au régime Covid check.* » Il y est précisé aussi que l'inscription sur cette liste doit être volontaire, qu'elle ne peut contenir que le nom des personnes vaccinées qui peuvent demander à voir retirer leur nom de ladite liste à tout moment sans aucune explication ou justification et que ladite liste doit être détruite au plus tard à l'expiration de la durée de la présente loi.

Avant d'analyser l'article précité, la CNPD tient à formuler trois remarques :

- Étant donné que le terme « liste » n'est pas prévu dans le RGPD, la Commission nationale suppose que les auteurs du projet de loi n° 7924 visent la tenue d'un fichier défini à l'article 4. point 6) du RGPD, que ce soit sous forme papier ou informatisée, comme « *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.* »

La CNPD propose ainsi auxdits auteurs d'adapter la terminologie en ce sens.

- La CNPD constate qu'en l'état actuel, le projet de loi n° 7924 sous avis ne permet qu'aux exploitants et organisateurs de tenir un fichier (« liste ») des personnes vaccinées et, a contrario, ne prévoit pas cette possibilité pour l'employeur qui a décidé de placer son entreprise ou administration sous le régime Covid check conformément à l'article 3septies de la loi modifiée du 17 juillet 2020. Or, en considérant que la disposition légale prévoyant qu'à partir du 15 janvier 2022, le régime 3G sera obligatoire sur le lieu de travail est en cours de finalisation et que le législateur vise à prévoir que l'employeur pourra établir et tenir une liste reprenant, sur une base volontaire, le nom des personnes vaccinées et rétablies,³⁵⁴ la CNPD analysera déjà ce volet dans le présent avis.
- Le projet de loi prévoit actuellement que les exploitants et organisateurs peuvent seulement tenir un fichier (« liste ») des personnes vaccinées. Or, la CNPD se demande dans ce contexte pourquoi les auteurs du projet de loi n° 7924 n'ont pas envisagé d'y faire figurer aussi les personnes rétablies.

Quant à la base légale

Il convient encore de préciser que la collecte d'information relatives au statut vaccinal d'une personne concernée (c'est-à-dire l'information selon laquelle la personne est ou non vaccinée) constitue un traitement de catégories particu-

³⁵⁴ Voir sur le site de la Chambre des députés, article "PREMIER ÉCHANGE SUR LA LOI COVID" du 6 décembre 2021: <https://chd.lu/wps/portal/public/Accueil/Actualite/ALaUne/?current=true&urille=wcm%3Apath%3AAactualite.public.chd.lu/ST-www.chd.lu/sa-actualites/11cbf556-a029-48ae-a2ed-9e892699c377>

lières de données à caractère personnel, dites « données sensibles », notamment de données de santé, qui est interdit en vertu du paragraphe (1) de l'article 9 du RGPD, sauf si une des conditions visées au paragraphe (2) dudit article est remplie. En plus du respect de l'article précité, le traitement de données sensibles doit se baser sur un des critères de licéité prévus à l'article 6 du RGPD.

La CNPD comprend du libellé du nouveau point 27 de l'article 1^{er} de la loi modifiée du 17 juillet 2020 que les « *personnes vaccinées lorsque celles-ci accèdent régulièrement à un établissement donné ou participent régulièrement à des activités ou événements soumis au régime Covid check* » peuvent consentir expressément à figurer sur une liste des personnes vaccinées, c'est-à-dire que la condition prévue à l'article 9.2.a) du RGPD s'appliquerait dans ce cas et que ce traitement se baserait en sus sur l'article 6.1.a) du RGPD. Elle recommande ainsi aux auteurs du projet de loi n° 7924 de se référer à ces dispositions du RGPD dans le corps du texte du projet de loi.

La CNPD tient à rappeler que dans cette hypothèse, il est important que ce consentement soit « *libre, spécifique, éclairée et univoque* » (article 4 point 11 du RGPD) et que les conditions applicables au consentement prévues à l'article 7 du RGPD soient respectées.

Par ailleurs, comme il ressort des travaux de la Commission de la Santé de la Chambre des Députés que l'employeur pourra « *établir et tenir une liste reprenant, sur une base vo-*

lontaire, le nom des personnes vaccinées et rétablies »³⁵⁵, la CNPD tient à attirer l'attention des auteurs du projet de loi sous examen sur le fait que le consentement n'est en principe pas une base de licéité adéquate pour des traitements mis en œuvre par un employeur concernant ses employés étant donné la relation de dépendance qui, sauf cas exceptionnels, entache le caractère libre dudit consentement. Il revient à l'employeur de démontrer que le traitement est valable dans ce cas exceptionnel, notamment en prouvant que les personnes disposent d'une véritable liberté de choix, c'est-à-dire qu'elles ont la possibilité de refuser sans subir de préjudice (considérant 42 du RGPD). En pratique, l'employeur devra donc toujours permettre aux employés qui ne souhaitent pas utiliser cette possibilité de figurer dans un fichier (« liste »), de présenter leur certificat à chaque fois qu'ils rentrent dans des zones placées sous régime Covid check, sans qu'ils ne subissent aucune conséquence négative de ce choix.

Quant à la finalité poursuivie

L'article 5.1.b) du RGPD exige que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités.

De la lecture de l'alinéa 4 du nouveau point 27 de la loi modifiée du 17 juillet 2020, la CNPD conclut que la finalité prévue par les auteurs du projet de loi sous avis par la tenue d'un fichier (« liste ») des personnes vaccinées par les

³⁵⁵ Voir sur le site de la Chambre des députés, article "PREMIER ÉCHANGE SUR LA LOI COVID" du 6 décembre 2021: <https://chd.lu/wps/portal/public/Accueil/Actualite/ALaUne/?current=true&urile=wcm%3Apath%3Aactualite.public.chd.lu/ST-www.chd.lu/sa-actualites/11cbf556-a029-48ae-a2ed-9e892699c377>

6

ANNEXES

exploitants et organisateurs est de « *faciliter les vérifications effectuées dans le cadre du Covid check.* » Il ressort par ailleurs des premiers échanges de la Commission de la Santé de la Chambre des Députés sur le projet de loi n°7924 que le fichier (« liste ») tenu par l'employeur reprenant, sur une base volontaire, le nom des personnes vaccinées et rétablies permettra à ces derniers « *de ne pas devoir, à chaque fois qu'ils accèdent au lieu de travail, se soumettre aux vérifications exhaustives imposées généralement dans le cadre du Covid-Check.* »³⁵⁶

Néanmoins, la CNPD a des doutes sur l'efficacité de la tenue d'un tel fichier (« liste »), que ce soit sur le lieu du travail ou lors d'activités de loisirs (secteur de l'Horeca, activités sportives, activités culturelles, etc) par rapport au but réellement poursuivi. Elle a du mal à s'imaginer que les personnes qui figurent sur un tel fichier (« liste ») ne soient plus contrôlées lorsqu'elles entrent dans le périmètre d'un Covid check seulement parce qu'elles figurent sur un fichier (« liste »). En effet, la personne responsable de scanner les codes QR dans le cadre du régime 2G ou 3G devrait tout au moins vérifier que la personne qui se présente à l'entrée figure bien dans le fichier (« liste »).

La CNPD se demande dans ce contexte si en pratique il est vraiment plus rapide de devoir rechercher les noms des personnes dans un fichier (« liste »), que de scanner rapidement le code QR moyennant l'application CovidCheck. lu et de vérifier que le quadrant devient vert. Surtout dans des grandes entreprises, admi-

nistrations ou lors d'évènements d'une certaine envergure, les personnes responsables des vérifications nécessaires dans le cadre du Covid check ne connaissent pas forcément toutes les personnes qui se présentent à l'entrée d'une zone Covid check. Elle se demande même si les exploitants et organisateurs seraient alors obligés de demander une pièce d'identité à la personne concernée afin de s'assurer qu'elle figure bien dans le fichier (« liste ») des personnes vaccinées ou, le cas échéant rétablies?

Par ailleurs, elle estime que pour faciliter le besoin d'entrées / sorties fréquentes au cours d'un laps de temps court (par exemple une journée) d'une zone Covid check, comme par exemple lors d'activités sportives ou culturelles qui sont ponctuelles, il existe des moyens moins intrusifs, sans collecte de données à caractère personnel, pour répondre à un besoin de facilitation des entrées / sorties d'une zone Covid check, comme par exemple l'usage de bracelets de couleur ou d'autres moyens de ce genre.

En ce qui concerne le système du Covid check sur le lieu du travail, la CNPD estime que pour les employés qui ont donné leur consentement explicite à figurer dans le fichier (« liste ») des personnes vaccinées et rétablies, certains employeurs pourraient envisager d'intégrer la durée de validité du certificat dans le badge d'accès des employés concernés, qui serait valable pendant cette durée ou jusqu'à la fin de la durée d'application des dispositions relatives au Covid check dans la loi modifiée du 17

³⁵⁶ Voir sur le site de la Chambre des députés, article "PREMIER ÉCHANGE SUR LA LOI COVID" du 6 décembre 2021: <https://chd.lu/wps/portal/public/Accueil/Actualite/ALaUne/?current=true&urille=wcm%3Apath%3AAactualite.public.chd.lu/ST-www.chd.lu/sa-actualites/11cbf556-a029-48ae-a2ed-9e892699c377>

juillet 2020. Si ce moyen faciliterait les vérifications effectuées dans le cadre du Covid check, l'accès serait facilité aux employés en cause sans nécessité de contrôle supplémentaire.³⁵⁷

Or, le fait d'intégrer cette information dans le badge d'accès des employés suppose toutefois un traitement de données supplémentaire, qui devrait respecter l'ensemble des principes et obligations du RGPD. A titre d'exemple, comme ce traitement a comme condition de licéité le consentement exprès des personnes concernées (article 9.2.a) RGPD), l'employeur devrait toujours permettre aux employés qui ne souhaitent pas utiliser cette possibilité de présenter leur certificat à chaque fois qu'ils rentrent dans des locaux placés sous régime CovidCheck, sans qu'ils ne subissent aucune conséquence négative de ce choix.

Quant aux données à caractère personnel collectées

Le nouveau point 27, alinéa 4 de l'article 1er de la loi modifiée du 17 juillet 2020 prévoit qu'actuellement le fichier (« liste ») des exploitants ou organisateurs ne peut contenir que « *le nom des personnes vaccinées* ».

Sans préjudice de ses commentaires sous le point « 2.2. *Quant à la finalité poursuivie* », la CNPD estime qu'au moins le nom et le prénom de la personne vaccinée ou rétablie devraient figurer dans ledit fichier (« liste ») afin d'éviter le risque lié aux homonymes.

Par ailleurs, la CNPD note que la durée de validité du certificat de vaccination, voire du certificat de rétablissement ne figure pas parmi les données à intégrer dans les fichiers (« listes ») en cause. Or, la CNPD se demande comment les finalités pour des raisons sanitaires pourraient être atteintes, si le certificat de vaccination ou de rétablissement d'une personne perdait sa validité entre la date d'entrée en vigueur et la date d'expiration de la loi du 17 juillet 2020 telle que modifiée par le présent projet de loi, c'est-à-dire le 28 février 2022.

Dès lors, si la personne qui s'occupe des vérifications liées au régime Covid check ne dispose pas de cette information et ne peut donc pas contrôler si la personne qui se trouve dans le fichier (« liste ») dispose encore d'un certificat valide, le but même du Covid check, c'est-à-dire de garantir la sécurité et la santé des personnes concernées sans devoir se soumettre aux restrictions et mesures sanitaires strictes, telles que le port du masque ou la distanciation physique, ne serait pas atteint.

Quant à d'autres obligations prévues par le RGPD

Finalement, l'employeur, l'exploitant ou l'organisateur qui tient un fichier (« liste ») des personnes vaccinées ou rétablies est à considérer comme responsable du traitement au sens de l'article 4. point 7) du RGPD et de ce fait, tous les principes et obligations prévus par le RGPD sont à respecter, comme par exemple :

³⁵⁷ Voir aussi les « FAQ SUR LA PROTECTION DES DONNÉES ET LE COVIDCHECK » disponible sur le site internet de la CNPD : <https://cnpd.public.lu/fr/dossiers-thematiques/covid-19/covid-check.html>.

6

ANNEXES

- Seul un nombre limité de personnes, dûment autorisées, pourra accéder audit fichier (« liste »).
Ainsi décidé à Belvaux en date du 8 décembre 2021.
- La sécurité et la confidentialité du fichier (« liste ») doit être garantie. Il importe que dans des lieux accessibles au public, ledit fichier (« liste ») ne puisse pas être visualisé par d'autres visiteurs ou clients.
La Commission nationale pour la protection des données
Tine A. Larsen
Présidente
- Les droits des personnes concernées, c'est-à-dire en l'espèce les personnes vaccinées et rétablies qui figurent dans un tel fichier (« liste »), prévus aux articles 12 à 23 du RGPD sont à respecter par le responsable du traitement.
Thierry Lallemand
Commissaire
Christophe Buschmann
Commissaire
Marc Lemmer
Commissaire

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7924 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19. (Délibération n° 53/AV31/2021 du 8/12/2021)

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 courriel en date du 4 décembre 2021, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur le projet de loi n° 7924 portant modification de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19³⁵⁸ (ci-après le « projet de loi n° 7924 »).

D'après l'exposé des motifs, en raison de la situation épidémiologique très préoccupante et de l'évolution du contexte sanitaire sur plusieurs fronts, le projet de loi n° 7924 « *se propose d'apporter des modifications substantielles à la version actuelle de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 qui vient, en principe, à échéance le 18 décembre 2021. Pour des raisons de santé et de sécurité des citoyens, il est d'ailleurs proposé de ne pas attendre cette échéance pour mettre en place les nouvelles mesures.* »

La CNPD constate dans ce contexte que les articles 5 et 10 de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 (ci-après : « loi modifiée du 17 juillet 2020 ») concernant notamment le traçage des contacts et le traitement de données à caractère personnel par la Direction de la santé à travers la mise en place d'un système d'information, n'ont pas subi de modifications.

³⁵⁸ Intitulé entier : « *Projet de loi n° 7924 portant modification: 1° de la loi modifiée du 17 juillet 2020 sur les mesures de lutte contre la pandémie Covid-19 ; 2° de la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des médicaments ; 3° de la loi modifiée du 6 janvier 1995 relative à la distribution en gros des médicaments ; 4° de la loi modifiée du 24 juin 2020 portant introduction de mesures temporaires relatives à la loi communale modifiée du 13 décembre 1988 et à la loi modifiée du 27 mars 2018 portant organisation de la sécurité civile dans le cadre de la lutte contre le Covid-19 ; 5° de la loi modifiée du 24 juin 2020 portant introduction d'une mesure temporaire relative à l'application de l'article 12 de la loi modifiée du 19 juillet 2004 concernant l'aménagement communal et le développement urbain dans le cadre de la lutte contre le Covid-19 ; 6° de la loi modifiée du 24 juin 2020 concernant la célébration du mariage dans un édifice communal autre que la maison communale dans le cadre de la lutte contre la pandémie Covid-19 ; 7° de la loi du 24 juillet 2020 portant dérogation temporaire aux articles L. 524-1, L. 524-2, L. 524-5, L. 541-1 et L. 541-2 du Code du travail ; 8° de la loi modifiée du 20 juin 2020 portant 1^{er} dérogation temporaire à certaines dispositions en matière de droit du travail en relation avec l'état de crise lié au Covid-19 ; 2^o modification du Code du travail ; 9° de la loi modifiée du 19 décembre 2020 portant dérogation temporaire à l'article L. 121-6 du Code du travail ; 10° de la loi modifiée du 19 décembre 2020 ayant pour objet la mise en place d'une contribution temporaire de l'Etat aux coûts non couverts de certaines entreprises ; 11° de loi modifiée du 19 décembre 2020 ayant pour objet la mise en place d'une nouvelle aide de relance ; 12° de la loi modifiée du 22 janvier 2021 portant : 1^{er} modification des articles L. 234-51, L. 234-52 et L. 234-53 du Code du travail ; 2^o dérogation temporaire aux dispositions des articles L. 234-5, L. 234-52 et L. 234-53 du Code du travail.* »

6

ANNEXES

Néanmoins, elle souhaite s'exprimer sur deux nouveautés intégrées dans le projet de loi sous avis impliquant des questions relatives à la protection des données, et plus spécifiquement sur l'obligation pour les exploitants d'établissements ou les organisateurs de rassemblements, de manifestations ou d'évènements (ci-après : « les exploitants et organisateurs ») sous régime Covid check de demander une pièce d'identité à la personne qui leur présente un certificat de vaccination ou de rétablissement, d'une part (1.), ainsi que sur la possibilité de tenir une liste des personnes vaccinées dans le cadre du Covid check par lesdits exploitants ou organisateurs, d'autre part (2.).

Quant à l'obligation de présenter une pièce d'identité dans le cadre du régime Covid check

Le nouveau point 27, alinéas 2 et 3 de l'article 1^{er} de la loi modifiée du 17 juillet 2020 entend modifier la définition du « régime Covid check » en prévoyant, entre autres, que « *l'exploitant de l'établissement ou l'organisateur du rassemblement, de la manifestation ou de l'évènement sous régime Covid check est tenu de demander une pièce d'identité à la personne qui lui présente un certificat de vaccination ou de rétablissement afin de s'assurer que l'identité mentionnée sur le certificat présenté et celle figurant sur la pièce d'identité sont identiques.* »

La CNPD comprend du libellé de l'article cité que les exploitants et organisateurs n'ont pas seulement la faculté, mais par contre une obligation de demander systématiquement une

pièce d'identité à la personne qui lui présente un certificat de vaccination ou de rétablissement afin d'éviter tout risque d'abus.

Les auteurs du projet de loi n° 7924 utilisent le terme « pièce d'identité », mais ne le définissent pas, de sorte qu'il faut partir du principe que les personnes concernées ne doivent pas forcément montrer leur carte d'identité, mais que tout autre document d'identité est susceptible de servir comme pièce d'identité, à savoir passeport, permis de conduire ou autres. Or, sans définir le terme pièce d'identité, il n'est pas aisé d'apprécier l'étendue dudit terme et posera des problèmes en pratique pour ceux qui sont obligés de mettre en œuvre cette disposition légale.

Par ailleurs, il y a lieu de rappeler que le RGPD n'a vocation à s'appliquer que lorsqu'un traitement de données à caractère personnel³⁵⁹ est effectué. Le simple fait que les exploitants et organisateurs visionnent les données à caractère personnel figurant sur une pièce d'identité ne constitue pas un traitement de données au sens du RGPD. Il en irait autrement si les exploitants et organisateurs étaient amenés à créer un fichier reprenant l'ensemble des données figurant sur les pièces d'identité des personnes contrôlées ou contenant des copies des pièces d'identité. En effet, en l'état actuel du droit, et sauf si un texte légal en prévoit expressément la possibilité, il s'agirait alors d'un traitement de données disproportionné, qui ne respecterait pas le principe de minimisation des données, dans la mesure où des moyens moins attentatoires à la vie privée des

³⁵⁹ Voir la définition du traitement de données prévu à l'article 4.2 du RGPD, ainsi que son champ d'application matériel prévu à l'article 2.1 du RGPD.

personnes concernées pourraient être mis en œuvre afin d'atteindre la finalité prévue, c'est-à-dire s'assurer par un contrôle visuel de ladite pièce que l'identité mentionnée sur le certificat présenté correspond bien à celle figurant sur la pièce d'identité.

Quant à la possibilité de tenir une liste des personnes vaccinées

Le nouveau point 27, alinéa 4 de l'article 1er de la loi modifiée du 17 juillet 2020 prévoit par ailleurs que pour « *faciliter les vérifications effectuées dans le cadre du Covid check, tout exploitant ou organisateur peut tenir une liste des personnes vaccinées lorsque celles-ci accèdent régulièrement à un établissement donné ou participent régulièrement à des activités ou événements soumis au régime Covid check.* » Il y est précisé aussi que l'inscription sur cette liste doit être volontaire, qu'elle ne peut contenir que le nom des personnes vaccinées qui peuvent demander à voir retirer leur nom de ladite liste à tout moment sans aucune explication ou justification et que ladite liste doit être détruite au plus tard à l'expiration de la durée de la présente loi.

Avant d'analyser l'article précité, la CNPD tient à formuler trois remarques :

- Étant donné que le terme « liste » n'est pas prévu dans le RGPD, la Commission nationale suppose que les auteurs du projet de loi n° 7924 visent la tenue d'un fichier défini à l'article 4. point 6) du RGPD, que ce soit sous forme papier ou informatisée, comme « *tout ensemble structuré de données à*

caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique. » La CNPD propose ainsi auxdits auteurs d'adapter la terminologie en ce sens.

- La CNPD constate qu'en l'état actuel, le projet de loi n° 7924 sous avis ne permet qu'aux exploitants et organisateurs de tenir un fichier (« liste ») des personnes vaccinées et, a contrario, ne prévoit pas cette possibilité pour l'employeur qui a décidé de placer son entreprise ou administration sous le régime Covid check conformément à l'article 3septies de la loi modifiée du 17 juillet 2020. Or, en considérant que la disposition légale prévoyant qu'à partir du 15 janvier 2022, le régime 3G sera obligatoire sur le lieu de travail est en cours de finalisation et que le législateur vise à prévoir que l'employeur pourra établir et tenir une liste reprenant, sur une base volontaire, le nom des personnes vaccinées et rétablies,³⁶⁰ la CNPD analysera déjà ce volet dans le présent avis.
- Le projet de loi prévoit actuellement que les exploitants et organisateurs peuvent seulement tenir un fichier (« liste ») des personnes vaccinées. Or, la CNPD se demande dans ce contexte pourquoi les auteurs du projet de loi n° 7924 n'ont pas envisagé d'y faire figurer aussi les personnes rétablies.

Quant à la base légale

Il convient encore de préciser que la collecte d'information relatives au statut vaccinal d'une

³⁶⁰ Voir sur le site de la Chambre des députés, article "PREMIER ÉCHANGE SUR LA LOI COVID" du 6 décembre 2021: <https://chd.lu/wps/portal/public/Accueil/Actualite/ALaUne/?current=true&urile=wcm%3Apath%3Aactualite.public.chd.lu/ST-www.chd.lu/sa-actualites/11cbf556-a029-48ae-a2ed-9e892699c377>

6

ANNEXES

personne concernée (c'est-à-dire l'information selon laquelle la personne est ou non vaccinée) constitue un traitement de catégories particulières de données à caractère personnel, dites « données sensibles », notamment de données de santé, qui est interdit en vertu du paragraphe (1) de l'article 9 du RGPD, sauf si une des conditions visées au paragraphe (2) dudit article est remplie. En plus du respect de l'article précité, le traitement de données sensibles doit se baser sur un des critères de licéité prévus à l'article 6 du RGPD.

La CNPD comprend du libellé du nouveau point 27 de l'article 1^{er} de la loi modifiée du 17 juillet 2020 que les « *personnes vaccinées lorsque celles-ci accèdent régulièrement à un établissement donné ou participent régulièrement à des activités ou événements soumis au régime Covid check* » peuvent consentir expressément à figurer sur une liste des personnes vaccinées, c'est-à-dire que la condition prévue à l'article 9.2.a) du RGPD s'appliquerait dans ce cas et que ce traitement se baserait en sus sur l'article 6.1.a) du RGPD. Elle recommande ainsi aux auteurs du projet de loi n° 7924 de se référer à ces dispositions du RGPD dans le corps du texte du projet de loi.

La CNPD tient à rappeler que dans cette hypothèse, il est important que ce consentement soit « *libre, spécifique, éclairée et univoque* » (article 4 point 11 du RGPD) et que les conditions applicables au consentement prévues à l'article 7 du RGPD soient respectées.

Par ailleurs, comme il ressort des travaux de la Commission de la Santé de la Chambre des Députés que l'employeur pourra « *établir et tenir une liste reprenant, sur une base volontaire, le nom des personnes vaccinées et rétablies* »³⁶¹, la CNPD tient à attirer l'attention des auteurs du projet de loi sous examen sur le fait que le consentement n'est en principe pas une base de licéité adéquate pour des traitements mis en œuvre par un employeur concernant ses employés étant donné la relation de dépendance qui, sauf cas exceptionnels, entache le caractère libre dudit consentement. Il revient à l'employeur de démontrer que le traitement est valable dans ce cas exceptionnel, notamment en prouvant que les personnes disposent d'une véritable liberté de choix, c'est-à-dire qu'elles ont la possibilité de refuser sans subir de préjudice (considérant 42 du RGPD). En pratique, l'employeur devra donc toujours permettre aux employés qui ne souhaitent pas utiliser cette possibilité de figurer dans un fichier (« liste »), de présenter leur certificat à chaque fois qu'ils rentrent dans des zones placées sous régime Covid check, sans qu'ils ne subissent aucune conséquence négative de ce choix.

Quant à la finalité poursuivie

L'article 5.1.b) du RGPD exige que les données à caractère personnel soient collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement d'une manière incompatible avec ces finalités.

De la lecture de l'alinéa 4 du nouveau point 27 de la loi modifiée du 17 juillet 2020, la CNPD

³⁶¹ Voir sur le site de la Chambre des députés, article "PREMIER ÉCHANGE SUR LA LOI COVID" du 6 décembre 2021: <https://chd.lu/wps/portal/public/Accueil/Actualite/ALaUne/?current=true&urile=wcm%3Apath%3AAactualite.public.chd.lu/ST-www.chd.lu/sa-actualites/11cbf556-a029-48ae-a2ed-9e892699c377>

conclut que la finalité prévue par les auteurs du projet de loi sous avis par la tenue d'un fichier (« liste ») des personnes vaccinées par les exploitants et organisateurs est de « faciliter les vérifications effectuées dans le cadre du Covid check. » Il ressort par ailleurs des premiers échanges de la Commission de la Santé de la Chambre des Députés sur le projet de loi n°7924 que le fichier (« liste ») tenu par l'employeur reprenant, sur une base volontaire, le nom des personnes vaccinées et rétablies permettra à ces derniers « *de ne pas devoir, à chaque fois qu'ils accèdent au lieu de travail, se soumettre aux vérifications exhaustives imposées généralement dans le cadre du Covid-Check.* »³⁶²

Néanmoins, la CNPD a des doutes sur l'efficacité de la tenue d'un tel fichier (« liste »), que ce soit sur le lieu du travail ou lors d'activités de loisirs (secteur de l'Horeca, activités sportives, activités culturelles, etc) par rapport au but réellement poursuivi. Elle a du mal à s'imaginer que les personnes qui figurent sur un tel fichier (« liste ») ne soient plus contrôlées lorsqu'elles entrent dans le périmètre d'un Covid check seulement parce qu'elles figurent sur un fichier (« liste »). En effet, la personne responsable de scanner les codes QR dans le cadre du régime 2G ou 3G devrait tout au moins vérifier que la personne qui se présente à l'entrée figure bien dans le fichier (« liste »).

La CNPD se demande dans ce contexte si en pratique il est vraiment plus rapide de devoir rechercher les noms des personnes dans un fichier (« liste »), que de scanner rapidement le

code QR moyennant l'application CovidCheck. lu et de vérifier que le quadrant devient vert. Surtout dans des grandes entreprises, administrations ou lors d'évènements d'une certaine envergure, les personnes responsables des vérifications nécessaires dans le cadre du Covid check ne connaissent pas forcément toutes les personnes qui se présentent à l'entrée d'une zone Covid check. Elle se demande même si les exploitants et organisateurs seraient alors obligés de demander une pièce d'identité à la personne concernée afin de s'assurer qu'elle figure bien dans le fichier (« liste ») des personnes vaccinées ou, le cas échéant rétablies ?

Par ailleurs, elle estime que pour faciliter le besoin d'entrées / sorties fréquentes au cours d'un laps de temps court (par exemple une journée) d'une zone Covid check, comme par exemple lors d'activités sportives ou culturelles qui sont ponctuelles, il existe des moyens moins intrusifs, sans collecte de données à caractère personnel, pour répondre à un besoin de facilitation des entrées / sorties d'une zone Covid check, comme par exemple l'usage de bracelets de couleur ou d'autres moyens de ce genre.

En ce qui concerne le système du Covid check sur le lieu du travail, la CNPD estime que pour les employés qui ont donné leur consentement explicite à figurer dans le fichier (« liste ») des personnes vaccinées et rétablies, certains employeurs pourraient envisager d'intégrer la durée de validité du certificat dans le badge d'accès des employés concernés, qui serait

³⁶² Voir sur le site de la Chambre des députés, article "PREMIER ÉCHANGE SUR LA LOI COVID" du 6 décembre 2021: <https://chd.lu/wps/portal/public/Accueil/Actualite/ALaUne/?current=true&urile=wcm%3Apath%3Aactualite.public.chd.lu/ST-www.chd.lu/sa-actualites/11cbf556-a029-48ae-a2ed-9e892699c377>

6

ANNEXES

valable pendant cette durée ou jusqu'à la fin de la durée d'application des dispositions relatives au Covid check dans la loi modifiée du 17 juillet 2020. Si ce moyen faciliterait les vérifications effectuées dans le cadre du Covid check, l'accès serait facilité aux employés en cause sans nécessité de contrôle supplémentaire.³⁶³

Or, le fait d'intégrer cette information dans le badge d'accès des employés suppose toutefois un traitement de données supplémentaire, qui devrait respecter l'ensemble des principes et obligations du RGPD. A titre d'exemple, comme ce traitement a comme condition de licéité le consentement exprès des personnes concernées (article 9.2.a) RGPD), l'employeur devrait toujours permettre aux employés qui ne souhaitent pas utiliser cette possibilité de présenter leur certificat à chaque fois qu'ils rentrent dans des locaux placés sous régime CovidCheck, sans qu'ils ne subissent aucune conséquence négative de ce choix.

Quant aux données à caractère personnel collectées

Le nouveau point 27, alinéa 4 de l'article 1er de la loi modifiée du 17 juillet 2020 prévoit qu'actuellement le fichier (« liste ») des exploitants ou organisateurs ne peut contenir que « le nom des personnes vaccinées ».

Sans préjudice de ses commentaires sous le point « 2.2. Quant à la finalité poursuivie », la CNPD estime qu'au moins le nom et le prénom de la personne vaccinée ou rétablie devraient

figurer dans ledit fichier (« liste ») afin d'éviter le risque lié aux homonymes.

Par ailleurs, la CNPD note que la durée de validité du certificat de vaccination, voire du certificat de rétablissement ne figure pas parmi les données à intégrer dans les fichiers (« listes ») en cause. Or, la CNPD se demande comment les finalités pour des raisons sanitaires pourraient être atteintes, si le certificat de vaccination ou de rétablissement d'une personne perdait sa validité entre la date d'entrée en vigueur et la date d'expiration de la loi du 17 juillet 2020 telle que modifiée par le présent projet de loi, c'est-à-dire le 28 février 2022.

Dès lors, si la personne qui s'occupe des vérifications liées au régime Covid check ne dispose pas de cette information et ne peut donc pas contrôler si la personne qui se trouve dans le fichier (« liste ») dispose encore d'un certificat valide, le but même du Covid check, c'est-à-dire de garantir la sécurité et la santé des personnes concernées sans devoir se soumettre aux restrictions et mesures sanitaires strictes, telles que le port du masque ou la distanciation physique, ne serait pas atteint.

Quant à d'autres obligations prévues par le RGPD

Finalement, l'employeur, l'exploitant ou l'organisateur qui tient un fichier (« liste ») des personnes vaccinées ou rétablies est à considérer comme responsable du traitement au sens de l'article 4. point 7) du RGPD et de ce fait,

³⁶³ Voir aussi les « FAQ SUR LA PROTECTION DES DONNÉES ET LE COVIDCHECK » disponible sur le site internet de la CNPD : <https://cnpd.public.lu/fr/dossiers-thematiques/covid-19/covid-check.html>

tous les principes et obligations prévus par le RGPD sont à respecter, comme par exemple :

- Seul un nombre limité de personnes, dûment autorisées, pourra accéder audit fichier (« liste »).
- La sécurité et la confidentialité du fichier (« liste ») doit être garantie. Il importe que dans des lieux accessibles au public, ledit fichier (« liste ») ne puisse pas être visualisé par d'autres visiteurs ou clients.
- Les droits des personnes concernées, c'est-à-dire en l'espèce les personnes vaccinées et rétablies qui figurent dans un tel fichier (« liste »), prévus aux articles 12 à 23 du RGPD sont à respecter par le responsable du traitement.

Ainsi décidé à Belvaux en date du 8 décembre 2021.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

6

ANNEXES

**Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7805 portant création d'une carte de stationnement pour personnes handicapées et relatif au projet de règlement grand-ducal 1° fixant le modèle et le contenu de la carte de stationnement pour personnes handicapées ainsi que la demande et du certificat médical en vue de l'obtention de cette carte ; 2° modifiant le règlement grand-ducal modifié du 26 août 1993 relatif aux avertissements taxés, aux consignations pour contrevenants non-résidents ainsi qu'aux mesures d'exécution de la législation en matière de mise en fourrière des véhicules et en matière de permis à points.
(Délibération n° 55/AV33/2021 du 10 décembre 2021)**

Conformément à l'article 57, paragraphe 1^{er}, 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 1^{er} 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 courriers en date du 24 mars 2021, Monsieur le Ministre de la Mobilité et des Tra-

voux publics a invité la Commission nationale à se prononcer sur le projet n°7805 portant création d'une carte de stationnement pour personnes handicapées (ci-après le « projet de loi ») ainsi que sur le projet de règlement grand-ducal 1° fixant le modèle et le contenu de la carte de stationnement pour personnes handicapées ainsi que la demande et du certificat médical en vue de l'obtention de cette carte ; 2° modifiant le règlement grand-ducal modifié du 26 août 1993 relatif aux avertissements taxés, aux consignations pour contrevenants non-résidents ainsi qu'aux mesures d'exécution de la législation en matière de mise en fourrière des véhicules et en matière de permis à points (ci-après le « projet de règlement grand-ducal »).

Il ressort de l'exposé des motifs qu' « *[a] ctuellement, les carte de stationnement pour personnes handicapées sont réglementées par les dispositions du règlement grand-ducal du 31 janvier 2003 concernant la création et l'utilisation d'une carte de stationnement pour personnes handicapées* » et qu'en 2019 « *il était prévu de remplacer ledit règlement grand-ducal de 2003 par un nouveau règlement grand-ducal afin de moderniser le texte et de notamment introduire un nouveau modèle de la carte de stationnement plus difficile à falsifier* ». Toutefois, « *dans son avis du 22 octobre 2019 le Conseil d'Etat a soulevé que depuis la révision constitutionnelle intervenue en 2007 les principes relatifs à l'intégration sociale des citoyens atteint d'un handicap sont une matière réservée à la loi et que dès lors le pouvoir réglementaire ne*

dispose pas du pouvoir spontané de règlementer cette matière ».

Les auteurs du projet de loi précisent que « *le présent projet de loi et son règlement d'exécution sont mis à profit pour remplacer le règlement grand-ducal modifié du 31 janvier 2003* ».

Dès lors, le projet de loi « *a pour objet de porter création d'une carte de stationnement pour personnes handicapées et de fixer les modalités en vue de l'obtention et de l'utilisation de cette carte* » et le projet de règlement grand-ducal entend notamment fixer « *le modèle et le contenu de la carte de stationnement pour personnes handicapées et du certificat médical en vue de l'obtention de cette carte* ».

Le présent avis limitera ses observations aux questions ayant trait à la protection des données à caractère personnel, soulevées par les articles 2 et 7 du projet de loi et les articles 1 et 2 du projet de règlement grand-ducal.

I. Sur la banque de données visée à l'article 7 du projet de loi

L'article 7, alinéa 1 du projet de loi dispose que « *[I]es informations relatives aux cartes de stationnement délivrées prévues aux articles 1er et 6, les renseignements contenus sur ces*

cartes ainsi que les informations concernant les procédures administratives concernant ces cartes sont reprises dans une banque de données nationale relative aux cartes de stationnement pour personnes handicapées ».

D'après les alinéas 4 et 5 dudit article, le ministre ayant les Transports dans ses attributions (ci-après le « ministre ») en est le responsable du traitement, au sens de l'article 4, point 7) du RGPD, et le Centre des technologies de l'information de l'Etat (ci-après le « CTIE ») a la qualité de sous-traitant au sens de l'article 4, point 8) du RGPD.

En ce qui concerne la terminologie retenue par les auteurs du projet de loi, c'est-à-dire les termes « *banque de données* », la CNPD considère qu'il serait plus approprié de l'aligner à la terminologie retenue par le RGPD qui utilise les termes de « *fichier* » ou encore de « *traitement* » de données.

1. Remarques préliminaires

Tout d'abord, la Commission nationale se félicite que, du point de vue de la sécurité juridique, soit prévu, à l'alinéa 1, de l'article 7 du projet de loi, le principe de la création d'une « *banque de données nationale relative aux cartes de stationnement pour personnes handicapées* », conformément à l'article 6, paragraphe (3) du RGPD³⁶⁴.

³⁶⁴ L'article 6, paragraphe (3), du RGPD 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'Etat 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. » (...) 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; (...).

6

ANNEXES

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'Etat 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 Etat 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 énonce encore que « cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée « Cour de

justice ») et de la Cour européenne des droits de l'homme. ».

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, bien qu'il y ait lieu de féliciter les auteurs du projet de loi d'avoir précisé les catégories de données qui seraient traitées, ainsi que les finalités pour lesquelles celles-ci seraient traitées, ou encore la durée de conservation des données traitées, certains éléments ne sont pas (ou pas suffisamment) précisés dans le projet de loi.

La CNPD y reviendra plus en détails dans les développements ci-après.

2. Sur le traitement de catégories particulières de données

En vertu de l'article 7 du projet de loi, le ministre collectera « la décision du médecin-membre de la commission médicale ». La Commission nationale comprend de l'avis du Conseil d'Etat³⁶⁵ que la « commission médicale » visée par le projet de loi est celle prévue à l'article 90 de l'arrêté grand-ducal modifié du 23 novembre 1955 portant règlement de la circulation sur toutes les voies publiques.

³⁶⁵ Avis n°60593 du 16 juillet 2021 du Conseil d'Etat sur le projet de loi portant création d'une carte de stationnement pour personnes handicapées, document parlementaire n°7805/02.

Il ressort encore de l'article 2 du projet de règlement grand-ducal que le ministre collectera également le certificat médical, tel que visé à l'annexe 2 du projet de règlement grand-ducal.

Dans la mesure où les données contenues dans ces documents sont susceptibles d'être relatives à la santé du demandeur d'une carte de stationnement pour personnes handicapées, celles-ci sont à qualifier de catégories particulières de données, dites « données sensibles » au sens de l'article 9 du RGPD.

Or, de tels traitements requièrent une protection spécifique³⁶⁶ 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.

Dans le cas présent, la Commission nationale estime que les traitements de données visés aux articles 2 et 7 du projet de loi, pourraient reposer 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* » ou sur l'article 9, paragraphe (2), lettre h), du RGPD qui dispose que « *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 ».

Ainsi, les auteurs du projet de loi devraient particulièrement être attentifs aux « *mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée* » qui devraient être mises en œuvre par le responsable du traitement dans le cadre des traitements de « données sensibles », tels que visés à l'article 7 du projet de loi et à l'article 2 du projet de règlement grand-ducal.

3. Sur les catégories de données à caractère personnel

S'il y a lieu de féliciter les auteurs du projet de loi d'avoir énuméré à l'article 7, alinéa 3 du projet de loi, les catégories de données qui seraient collectées par le ministre, le texte sous avis omet de préciser certaines catégories de données ou demeure imprécis en ce qui concerne l'énumération de certaines catégories de données.

Par ailleurs, il est suggéré de supprimer la formulation suivante « *toutes les données nécessaires pour les finalités suivantes* » employée à l'alinéa 2, de l'article 7, du projet

³⁶⁶ 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.

6

ANNEXES

de loi, alors que les dispositions de l'alinéa 3 du même article, énumère limitativement les catégories de données qui seraient collectées.

En tout état de cause, une telle formulation est trop vague et ne serait pas susceptible de respecter le principe de minimisation des données en vertu duquel 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.

La CNPD propose ainsi de reformuler l'alinéa 2, de l'article 7 du projet de loi, de la manière suivante : « Les catégories de données à caractère personnel, visées à l'alinéa 3, sont collectées et traitées pour les finalités suivantes : (...) ».

A. Sur les données relatives aux établissements auxquels la carte de stationnement est délivrée

L'article 7, alinéa 3 du projet de loi dispose que « [d]ans cette banque de données figurent les données suivantes : (...) le nom, le matricule, le numéro d'identification du véhicule et l'adresse de contact de l'établissement auquel la carte de stationnement est délivrée ».

Il ressort des dites dispositions que des données concernant des personnes morales seraient susceptibles d'être collectées par le ministre.

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 à ce titre au ministre.

Par ailleurs, il y a lieu de s'interroger sur ce que recouvre le terme « *matricule* » visé par les dispositions précitées. S'agit-il du numéro d'enregistrement de l'établissement au Registre de Commerce et des Sociétés ?

Pour plus de clarté et une meilleure compréhension, les auteurs du projet de loi devraient veiller à utiliser la terminologie appropriée.

B. Sur les catégories de données collectées à travers les formulaires visés à l'annexe 2 du projet de règlement grand-ducal

Il y a lieu de relever que l'article 7, alinéa 3, point 1° du projet de loi ne reflète pas entièrement les catégories de données qui seraient collectées par le ministre à travers le formulaire de

« [d]emande pour l'obtention d'une carte de stationnement pour personnes handicapées à mobilité réduite »³⁶⁷, et le formulaire « *certificat médical* »³⁶⁸.

Or, l'alinéa 1, de l'article 7 du projet de loi précise que les « *informations concernant les procédures administratives concernant ces cartes sont reprises dans une banque de donnée nationale* ».

Ainsi, cela signifie-t-il que le numéro d'identification national qui figure sur le formulaire « [d]emande pour l'obtention d'une carte de stationnement pour personnes handicapées à mobilité réduite » et les données contenues dans le « *certificat médical* » ne seraient pas amenés à figurer dans le fichier ?

Il en va de même pour la photocopie du permis de conduire, cette pièce est à joindre par le requérant, si ce dernier en possède un, au formulaire « *certificat médical* » mais l'article 7, alinéa 3 du projet de loi ne fait référence qu'au numéro du permis de conduire.

Si de telles données sont effectivement amenées à figurer dans le fichier précité, le texte sous avis devrait expressément le refléter.

En outre, la CNPD se demande si les données relatives à la « *signalétique* » du titulaire de la carte, visées à l'article 7, alinéa 3, point 1^o du projet de loi, englobent les nom, prénom, numéro de téléphone et e-mail de la personne requérante, que cette dernière doit communiquer au ministre lorsqu'elle lui soumet une

demande de carte de stationnement ? Si tel ne devait pas être le cas, la Commission nationale se demande quelles données seraient visées par la « *signalétique* » du titulaire de la carte, visées à l'article 7, alinéa 3, point 1^o du projet de loi.

Dans tous les cas, et pour une meilleure compréhension du texte sous avis, il est proposé de remplacer le terme « *signalétique* » par une liste exacte des données que le responsable du traitement est amené à traiter.

Par ailleurs, il y a lieu de constater que les données relatives à la date et lieu de naissance ne figurent pas comme catégories de données qui seraient amenées à figurer dans le fichier. Or, celles-ci sont collectées lors de la demande de la carte de stationnement soumise au ministre. Si de telles données devaient figurer dans ledit fichier alors cela devrait être reflété dans le dispositif sous avis.

Enfin, en l'absence de précisions dans le commentaire des articles sur les raisons qui justifieraient la collecte du numéro d'identification national (« *matricule* ») et de la photocopie du permis de conduire, la CNPD n'est pas en mesure d'apprécier si le principe de minimisation des données, en vertu duquel seules les données nécessaires à la réalisation des finalités doivent être traitées, serait respecté. Il en va de même pour la photo du demandeur de la carte. Bien que l'article 7, alinéa 3, point 2^o du projet de loi sous avis ainsi que le formulaire de « [d]emande pour l'obtention d'une carte de stationnement pour

³⁶⁷ Voir annexe 2 du projet de règlement grand-ducal.

³⁶⁸ Voir annexe 2 du projet de règlement grand-ducal.

6

ANNEXES

personnes handicapées à mobilité réduite »³⁶⁹ prévoit cette collecte, il y a lieu de constater que la nécessité des traitements de cette donnée à caractère personnel n'est pas justifiée par les auteurs du projet de loi. Le spécimen de la carte de stationnement pour personnes physiques annexé au projet de règlement grand-ducal contient un emplacement pour apposer la photo fournie et les auteurs précisent qu'ils ont recouru au spécimen mis à disposition par l'Union européenne. Si dès lors, la fourniture de la photo se fonde sur une contrainte découlant du droit de l'Union européenne, les auteurs du projet de loi devraient le préciser.

En outre, il y a lieu de rappeler que l'utilisation du numéro d'identification national est, en principe, encadré par la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques.

C. Sur la collecte de la « décision du médecin-membre de la commission médicale »

Selon le point 5°, de l'alinéa 3, de l'article 7 du projet de loi, le fichier contiendra également la « décision du médecin-membre de la commission médicale ».

En l'absence de précisions dans le commentaire des articles, la Commission nationale se demande quelles seraient les données qui seraient effectivement contenues dans cette décision. S'agit-il de la copie de l'intégralité de l'avis prévu à l'article 2, alinéa 1^{er} du projet de loi, ou de la copie du résultat de l'examen médical, auquel

doit éventuellement se soumettre le demandeur en vertu de l'article 2, alinéa 3 du projet sous avis, voire des deux ?

Conformément au principe de minimisation des données prévu à l'article 5, paragraphe 1er, lettre c), du RGPD, la CNPD estime, en tout état de cause, que seul un avis « négatif » ou « positif » de la part du médecin-membre de la commission médicale, en ce qui concerne la délivrance de la carte de stationnement, devrait être communiqué au ministre. Dès lors, cet avis ne devrait pas contenir des données de santé du demandeur de la carte de stationnement.

4. Sur l'accès aux données à caractère personnel

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)* ».

En outre, 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

³⁶⁹ Voir annexe 2 du projet de règlement grand-ducal.

non-autorisés aux données ou des fuites de données.

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. Dans ce contexte, il est vivement recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début les personnes ou le service compétent qui auraient accès aux données ou à l'interface informatique mise à disposition par le CTIE, et à quelles données précises ces personnes ou ce service aurait accès. Ce d'autant plus dans la mesure où des « données sensibles » sont amenées à être traitées.

Le ministre devra ainsi mettre en place de telles mesures 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.

Sur ce dernier point, la CNPD recommande que les données de journalisation soient conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.

La Commission nationale souligne aussi l'importance d'effectuer pro activement des contrôles en interne. A cet effet, il convient conformément à l'article 32, paragraphe (1), lettre d) du RGPD de mettre en œuvre une procédure « *visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».

Ainsi, s'il y a lieu de féliciter les auteurs du projet de loi d'avoir prévu à l'article 7, alinéa 6 du projet de loi que « *[l]'accès aux données et la possibilité de les traiter sont gérés par un système de gestion des identités et des droits d'accès* », il est important que le responsable du traitement veille à ce que ce système de gestion des identités et des droits d'accès respectent les considérations formulées ci-avant, en l'absence de plus de précisions quant aux modalités de ce système.

5. Sur la durée de conservation des données à caractère personnel

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 (principe de la limitation de la conservation).

S'il y a lieu de féliciter les auteurs du projet de loi d'avoir prévu des durées de conservations pour les données traitées dans le cadre du projet

6

ANNEXES

de loi et du projet de règlement grand-ducal, des précisions mériteraient néanmoins d'être apportées.

Ainsi, l'article 7, alinéa 7 du texte sous avis tel qu'amendé par les amendements parlementaires du 26 octobre 2021 entend prévoir une durée de conservation de trois mois, à partir de l'émission de la carte de stationnement, pour la photographie et la signature du titulaire et une durée de dix ans pour les « autres données ».

L'article 7, alinéa 8 du projet de loi tel qu'amendé par les amendements parlementaires du 26 octobre 2021 prévoit encore une dérogation au délai de conservation de 10 ans pour les données des titulaires de cartes de stationnement permanentes pour lesquelles les données « peuvent être conservées au-delà d'une durée de dix ans ».

En ce qui concerne la dérogation prévue à l'alinéa 8 précité, les auteurs du projet de loi précisent qu'« [a]fin d'éviter aux personnes avec des handicaps permanents de devoir joindre un certificat récent attestant le handicap lors du renouvellement de leur carte, il y a lieu de conserver ces informations. A titre d'exemple, une personne ayant perdu une jambe devrait au cas contraire joindre un certificat médical attestant la perte de la jambe tous les 10 ans ». Dans la mesure où seules les données contenues dans le certificat médical semblent être visées, le texte sous avis devrait expressément le refléter.

En ce qui concerne les autres durées de conservation et bien que celles-ci soient fixées par lesdites dispositions, les auteurs du projet de loi dans leur commentaire des articles n'expliquent pas les critères retenus qui justifieraient de telles durées. Ces derniers se limitent, en effet, à indiquer que la durée de 3 mois a été fixée « en analogie à d'autres banques de données » et que la durée de conservation de 10 ans « correspond à la durée de validité de deux cartes de stationnement ».

Or, ces explications ne suffisent pas à justifier pourquoi la conservation desdites données pour de telles durées serait nécessaire et justifiée.

Ainsi, la Commission nationale se demande pourquoi les auteurs du projet de loi entendent fixer une durée de conservation de 10 ans qui correspond à « la durée de validité de deux cartes de stationnement », alors qu'une carte de stationnement est valide pendant 5 ans et qu'à l'issue de ces 5 années, celle-ci doit être renouvelée ?

Il y a encore lieu de s'interroger sur l'articulation des dispositions du projet de loi qui prévoient une durée de conservation de 10 ans pour « les autres données » à l'exception de la photographie et signature du titulaire d'une carte de stationnement, avec celles de l'article 2 du projet de règlement grand-ducal qui dispose que « [l]e certificat médical a une durée de validité de trois mois à compter de la date de délivrance par le médecin-examineur ».

Est-il nécessaire et justifié de conserver pendant une durée de 10 ans, un certificat médical qui ne sera valable que pour une durée de trois mois à compter de la date de délivrance par le médecin-examineur ?

Par conséquent, en l'absence de précisions, des auteurs du projet de loi dans le commentaire des articles précités quant aux critères qui justifieraient de telles durées, la Commission nationale n'est pas en mesure d'apprécier si en l'occurrence, le principe de durée de conservation limitée des données a été respecté, et invite les auteurs du projet de loi à fournir des précisions à cet égard.

En outre, il y a lieu de constater que la disposition sur les durées de conservation s'applique aux seules données contenues dans le fichier. En effet, la CNPD comprend que les demandes ainsi que les certificats médicaux et le cas échéant les photocopies des permis de conduire sont reçus en version papier et ensuite transcrits dans le fichier. Ainsi, il convient de se demander quelles durées de conservation sont prévues pour les données fournies sur papier, en particulier concernant les catégories particulières de données, dites « données sensibles » au sens de l'article 9 du RGPD, le numéro d'identification national ainsi que la photo du demandeur.

Enfin, il y a lieu de rappeler que le responsable du traitement doit en vertu de l'article 5, paragraphe (1), lettre d) du RGPD s'assurer que les données qu'il traite sont exactes et tenues à jour et prendre toutes les

mesures raisonnables « pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ».

II. Sur le QR code figurant sur la carte de stationnement pour personnes physiques

Selon l'exposé des motifs du projet de loi, le nouveau modèle de carte de stationnement est « plus difficile à falsifier ». L'exposé des motifs du projet de règlement grand-ducal précise à son tour qu' « il est profité de l'occasion pour adapter les modèles des cartes de stationnement afin de les protéger contre la falsification ou la contrefaçon » et qu' « à l'aide d'un lecteur de code QR, ce code permet à un appareil électronique de renseigner sur la nature du document ».

Le code QR servira donc à contrôler la véracité des cartes de stationnement.

La Commission nationale regrette que les modalités d'un tel contrôle, en pratique, ne soient pas précisées par les auteurs du projet de loi et du projet de règlement grand-ducal et se demande dès lors comment un tel contrôle se déroulera en pratique.

En effet, il y a lieu de se demander qui effectuera ces contrôles. Est-ce que sera le rôle des agents municipaux ou de la Police grand-ducale ? S'il n'y a aucun doute sur la compétence de la Police grand-ducale pour effectuer de tels

6

ANNEXES

contrôles, il en est autrement des agents municipaux.

Ainsi décidé à Belvaux en date du 10 décembre 2021.

En outre, la personne qui contrôlera la nature du document à l'aide d'un appareil électronique accèdera-t-elle directement à distance au fichier prévu à l'article 7 du projet de loi ?

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

En tout état de cause, la CNPD estime que ces personnes ne devraient avoir accès qu'aux informations relatives à la validité de la carte de stationnement, c'est-à-dire si la carte est en cours de validité ou non, à l'exclusion des autres données personnelles figurant dans ledit fichier. En aucun cas, ces dernières ne devraient avoir accès à l'intégralité des données contenues dans le fichier.

Thierry Lallemand
Commissaire

Christophe Buschmann
Commissaire

Marc Lemmer
Commissaire

CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

```
01100  
00101111  
11011011  
010001  
011000  
01000  
00010  
1101011011  
10110110001110  
1010001100110011  
11011000101110101  
01101000111001100  
10110001010101101  
11011101011010101  
010110110001110101  
1010001100110101  
1011000101110 0111  
01101000111001 001  
10110001010101 101  
010111010110110 000  
010110110001110 010  
010001100110010 01  
01000101110101110  
110100011100110010  
011000101010110101
```

15, Boulevard du Jazz - L-4370 Belvaux
Téléphone : +352 26 10 60-1 - info@cnpd.lu
www.cnpd.lu