RAPPORT ANNUEL 2024

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

RAPPORT ANNUEL 2024

CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

TABLE DES MATIÈRES

1 INTRODUCTION 4

2 AVANT-PROPOS 8

3 UNE ANNÉE EN CHIFFRES 16

4 LES ACTIVITÉS EN 2024 20

LES ACTIVITÉS DANS LE CADRE DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES 20

1 Sensibiliser le public 20
2 Répondre aux demandes d'information de particuliers et de professionnels 30
3 Intervenir dans le processus législatif 32
4 Guider les acteurs privés et publics 43
5 Désignation des délégués à la protection des données 47
6 Accompagner la mise en conformité 49
7 Traiter les réclamations des citoyens 70
8 Analyser les violations de données 75
9 Recevoir les signalements de type «whistleblowing» 80
10 Contrôler et adopter des mesures correctrices 81

LE CONTRÔLE DES TRAITEMENTS DE DONNÉES DES AUTORITÉS RÉPRESSIVES OU DE SÉCURITÉ NATIONALE 85

1 Demandes d'information 86
2 Avis 86
3 Réclamations 86
4 Notifications de violations de données 86

LES ACTIVITÉS DANS LE CADRE DE LA SUPERVISION COORDONNÉE DES SYSTÈMES D'INFORMATION À GRANDE ÉCHELLE DE L'UE ET DES ORGANES, OFFICES ET AGENCES EUROPÉENNES 87

1 Système d'information Schengen (SIS) 88

2 Système d'information sur les visas (VIS) 88

3 Europol 88

4 Mécanisme d'évaluation et de suivi de Schengen (SCHEVAL) 88

5 Avis 88

LA PROTECTION DE LA VIE PRIVÉE DANS LE SECTEUR DES COMMUNICATIONS ÉLECTRONIQUES **89**

1 Violations de données dans le secteur des communications électroniques 89

LES TRAVAUX INTERNATIONAUX DANS LE DOMAINE DE LA PROTECTION DES DONNÉES **90**

1 Comité européen pour la protection des données (EDPB ou European Data Protection Board) 90

2 Global Privacy Assembly 93

3 Conférence de printemps des autorités européennes à la protection des données (Spring Conference) 95

4 European Case Handling Workshop (ECHW) 95

5 Groupe de Berlin 96

6 Association francophone des autorités de protection des données personnelles (AFAPDP) 97

7 Comité de la Convention 108 (T-PD) du Conseil de l'Europe 97

5 RESSOURCES, STRUCTURES ET FONCTIONNEMENT 98

1 Ressources humaines 98

2 Organisation de la CNPD 103

3 Rapport de gestion relatif aux comptes de l'exercice 2023 104

6 ANNEXES 112

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

INTRODUCTION

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

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

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

- du Règlement général sur la protection des données ;
- de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données ;
- de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale ;
- de la loi modifiée du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques ;
- des textes légaux prévoyant des dispositions spécifiques en matière de protection des données à caractère personnel.

Elle n'est pas compétente pour contrôler les opérations de traitement de données à caractère personnel effectuées par les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif dans l'exercice de leurs fonctions juridictionnelles. Cette mission revient à l'autorité de contrôle de la protection des données judiciaires.

INTRODUCTION

MISSIONS

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

INFORMER ET GUIDER PAR LE BIAIS DE :

- la sensibilisation du public aux fins de favoriser 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 ;
- la promotion de codes de conduite, des schémas de certification et l'agrément des organismes de certification ;
- les recommandations aux responsables 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

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 le nombre potentiel d'individus affectés.

L'**expertise** est très importante pour la CNPD qui est dédiée à un travail de qualité. À 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.

AVANT-PROPOS

Le collège : Alain Herrmann, Thierry Lallemang, Tine A. Larsen et Marc Lemmer.

2

UNE ANNÉE SOUS LE SIGNE DE L'INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle (IA), autrefois confinée aux laboratoires de recherche, est désormais omniprésente dans notre quotidien. Des algorithmes sophistiqués analysent des montagnes de données pour nous offrir des recommandations personnalisées, tandis que des robots intelligents révolutionnent des industries entières.

Comme les technologies d'intelligence artificielle et en particulier leurs modèles d'apprentissage nécessitent des quantités considérables de données, et que de nombreuses applications se situent dans un contexte de personnalisation, la protection des données personnelles est devenue un sujet de préoccupation central.

Ayant développé ses compétences en matière d'IA au cours des dernières années, les choses se sont concrétisées pour la Commission nationale fin 2024 : elle a été proposée comme autorité compétente pour la mise en œuvre nationale de l'« AI Act ».

Qu'est-ce que cela signifie ?

Revenons un peu en arrière : Suite à l'ascension fulgurante de l'intelligence artificielle catalysée par le déploiement de ChatGPT en 2022, l'Union européenne a adopté le règlement « AI Act » le 13 mars 2024 pour promouvoir une IA digne de confiance tout en assurant le respect des droits fondamentaux des individus. La loi vise à réguler des produits d'intelligence artificielle qui sont commercialisés sur le marché européen. Depuis l'entrée en vigueur de ce règlement le 1er août 2024, les États membres sont dans l'obligation de préparer sa mise en œuvre, un des premiers aspects de laquelle est la désignation des autorités compétentes.

Le 29 novembre 2024, le gouvernement luxembourgeois a déposé le projet de loi visant à mettre en œuvre certaines dispositions de l'AI Act et désignant notamment les autorités compétentes au niveau national. La CNPD se verrait ainsi attribuer plusieurs rôles : le point de contact unique et la coordination nationale des autorités compétentes, autorité de surveillance du marché par défaut (supervision des systèmes d'IA de l'annexe III du règlement et des systèmes d'IA qui ne relèvent pas de la compétence des autorités sectorielles) et autorité en charge des droits fondamentaux (avec l'ALIA et l'ITM). Elle aurait également l'obligation de mettre en place un bac à sable règlementaire dans le cadre du règlement européen.

AVANT-PROPOS

Démystifier l'IA et responsabiliser les acteurs

La décision de proposer des rôles à la CNPD dans le contexte de l'AI Act n'est pas née du néant. La Commission nationale avait déjà acquis une certaine expertise dans le domaine qu'elle mettait au service des parties prenantes.

Le 24 mai 2024, elle a lancé le projet « Sandkëscht » (« bac à sable » en luxembourgeois). Il s'agit d'un environnement d'expérimentation sécurisé où les entreprises peuvent tester des innovations numériques, notamment celles appuyées par l'IA, par rapport à leur conformité au RGPD. Ce cadre fermé et contrôlé permet aux développeurs de collaborer étroitement avec la CNPD pour identifier et atténuer les risques liés à la protection des données dès les phases initiales de développement.

Cette initiative favorisant une approche « privacy-by-design » répond à une partie significative des besoins et questions que soulèvent les acteurs de la place en matière de l'IA et que la CNPD a pu rassembler au cours d'un appel à contributions public publié sur son site au début de l'année. En plus, la CNPD a identifié d'autres pistes d'action à exploiter.

S'inspirant du succès des sessions « Data Protection Basics » (DPB), la Commission nationale a développé la formation « Data Protection Basics for Artificial Intelligence » (DP4AI). Ce cours permet aux participants de se familiariser avec les concepts de base de l'IA tout en abordant les liens avec la gestion et la protection des données personnelles ainsi que l'interaction avec le RGPD. Lancé en décembre 2024, DP4AI continue de faire preuve d'une popularité remarquable.

En parallèle, la CNPD a entrepris en 2024 l'organisation de six ateliers de travail « DaProLabs » pour aborder un nombre de questions concernant l'intelligence artificielle et la protection des données. S'adressant aux professionnels de la protection des données ainsi qu'aux experts en matière de l'intelligence artificielle, les ateliers favorisaient l'échange de connaissances, d'expériences et de bonnes pratiques en la matière.

En outre, la CNPD s'est activement saisie des questions liées à l'IA tout au long de l'année, participant à des événements sur le sujet, comme la conférence « L'intelligence artificielle : aspects juridiques et enjeux pratiques pour les entreprises » organisée par la Chambre de Commerce, la conférence « AI Act: impacts for the financial sector? » organisée par l'Association des Banques et Banquiers du Luxembourg (ABBL) et Arendt, la table ronde intitulée « Naviguer vers l'Avenir : Mise en Œuvre et Régulation de l'Intelligence Artificielle (IA) », ainsi que la conférence « Intelligence Artificielle et Protection des données »

organisée par l'Association pour la Protection des Données au Luxembourg (APDL).

Au niveau européen, l'European Data Protection Board (EDPB) a publié plusieurs avis concernant l'utilisation des données personnelles dans le développement et le déploiement des modèles d'IA. L'un des avis clés, adopté en décembre 2024, examine les conditions dans lesquelles un modèle d'IA peut être considéré comme anonyme, l'utilisation de l'intérêt légitime comme base juridique, et les conséquences d'un traitement illégal des données personnelles.

Une année pleine de jalons

Bien que l'intelligence artificielle a été le sujet phare des activités de la CNPD en 2024, la Commission nationale a connu d'autres moments remarquables au cours de l'année.

Le lancement officiel de DAAZ (« Data Accountability from A to Zen ») en juin 2024 a marqué une nouvelle étape dans la promotion d'une meilleure compréhension des principes de la protection des données. La plateforme en ligne, développée dans le cadre d'un projet cofinancé par l'Union Européenne, aide les PME et start-ups à se conformer au RGPD dans leurs activités quotidiennes et connaît un grand succès même au-delà des frontières luxembourgeoises.
Fin 2024, l'avis de la CNPD sur le projet de loi n°8395 concernant la mise en œuvre du principe « once only » dans le cadre du Data Governance Act (DGA) a été un jalon majeur dans les débats sur la protection des données au Luxembourg. Le principe « once only » vise à éviter que les citoyens et entreprises aient à fournir plusieurs fois les mêmes informations aux administrations publiques, en facilitant le partage sécurisé des données entre autorités. Cet avis s'est particulièrement attaché à définir les garanties nécessaires pour assurer une utilisation responsable et sécurisée des données personnelles dans les échanges administratifs.

La CNPD a également mis en ligne un canal pour les lanceurs d'alerte, offrant une plateforme sécurisée pour signaler les violations de la protection des données. Ce canal permet aux individus de signaler anonymement des pratiques non conformes, renforçant ainsi la transparence et la responsabilité au sein des organisations.

La Commission nationale a co-organisé l'inauguration du bâtiment Twist en septembre 2024, nouveau siège du STATEC qui abrite une annexe de la CNPD. Les nouveaux bureaux offrent des installations modernes et adaptées aux besoins croissants de la Commission, permettant une meilleure gestion des ressources et une efficacité accrue dans la réalisation de ses missions.

AVANT-PROPOS

Inauguration du bâtiment Twist en septembre 2024.

Autres moments forts de l'année précédente étaient sans doute la visite de Madame la ministre Elisabeth Margue et l'audience des membres du Collège auprès de S.A.R. le Grand-Duc Héritier. Renforçant les liens institutionnels, ces visites soulignent l'importance de la CNPD dans le paysage institutionnel luxembourgeois et de sa guidance en matière de protection des données personnelles.

Guidance, contrôle, sensibilisation

La préparation à ces nouvelles responsabilités ne signifiait pas que la CNPD pouvait consacrer moins de temps à ses tâches habituelles. A ce titre, la Commission nationale a publié 32 avis en 2024 relatifs à des projets ou propositions de loi ou mesures réglementaires portant par exemple sur le carnet de vaccination électronique,

Visite de Madame la ministre Elisabeth Margue.

Audience des membres du Collège auprès de S.A.R. le Grand-Duc Héritier.

AVANT-PROPOS

le système d'information Schengen et la signature électronique des actes.

La CNPD a également publié son « premier retour d'expérience sur la protection des données, numérisation et innovation au Luxembourg », mettant en lumière les avancées réalisées et les domaines nécessitant encore des améliorations, fournissant une base solide pour les futures initiatives de la CNPD et repris entre autres dans son programme de travail 2025.

2024 était aussi marqué par la publication d'un bilan des activités de surveillance dans le contexte de la pandémie Covid-19, soulignant les défis uniques posés par la crise sanitaire et proposant des recommandations pour améliorer la résilience des systèmes de gestion des données en période de crise.

La Commission nationale a reçu 594 demandes de renseignement par écrit en 2024, concernant surtout la surveillance sur le lieu de travail, les ressources humaines et le droit des personnes concernées. 516 réclamations lui ont été soumises la même année, ainsi que 442 notifications de violations de données signalées. Les raisons principales en étaient respectivement le non-respect de droits et l'erreur humaine.

À la fin de l'année 2024, la division Enquêtes a géré 44 dossiers actifs, dont 29 ouverts en 2024. Les contrôles récurrents sur la vidéosurveillance dans les lycées et les registres des traitements ont conduit à 10 enquêtes. Plusieurs enquêtes réactives ont aussi été ouvertes sur des sujets comme le droit d'accès et la prospection commerciale. Les alertes reçues, provenant des divisions Réclamations et Guidance, ont porté sur des problématiques variées, notamment les failles de sécurité et le recueil du consentement.

L'année dernière, la CNPD a organisé ou participé à 48 formations et conférences, y inclus le PwC Cybersecurity & Privacy Day, le Printemps des DPO à Paris, le Forum International de la Cybersécurité à Lille, la « Privacy Symposium Conference » à Venise, la conférence de la Global Privacy Assembly à Jersey ou encore, à Luxembourg, le « Symposium sur la cybersécurité et la protection des données dans l'action humanitaire ».

Et n'oublions pas la campagne de sensibilisation « Vos données, vos droits ! » lancée en janvier 2024 pour rappeler au public ses droits en matière de protection des données en 2024. Cette campagne vise à renforcer la compréhension et la vigilance des citoyens concernant la protection de leurs informations personnelles.

De nouveaux repères pour une autorité en évolution

La CNPD intervient dans tous les secteurs d'activité dès lors que des données

2

personnelles sont en jeu. Cette portée étendue lui confère une vision globale des défis associés au développement numérique, mais engendre également des attentes et une responsabilité à la hauteur de cette ampleur.

La CNPD reste déterminée à relever les défis de la protection des données personnelles et à promouvoir une culture de respect et de sécurité des informations privées. Je tiens à remercier tous nos collaborateurs pour leur engagement et tous nos partenaires pour leur soutien continu envers la protection des données. Ensemble, nous continuerons à œuvrer pour un environnement numérique sûr et respectueux des droits de chacun.

Tine A. Larsen
Présidente

UNE ANNÉE EN CHIFFRES

SENSIBILISATION, GUIDANCE ET CONSEILS

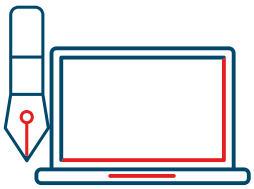
32

AVIS

par rapport à 44 en 2023

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

- Règlement sur les services numériques
- Carnet de vaccination électronique
- Rétention des données
- Système d'information Schengen
- Signature électronique des actes
- Traitement de données concernant la santé en matière d'assurance et de réassurance
- Fiches d'hébergement
- Plateforme de données énergétiques
- Sécurité, sûreté, ordre et vidéosurveillance dans les transports publics
- Échange de données électorales entre États membres de l'UE
- Police grand-ducale



594

DEMANDES DE RENSEIGNEMENT PAR ÉCRIT

par rapport à 691 en 2023

Les 3 principales catégories de demandes concernent :

- la surveillance sur le lieu de travail ;
- les ressources humaines ;
- le droit des personnes concernées (droit d'accès, droit à l'effacement, etc.).

48

FORMATIONS ET CONFÉRENCES

par rapport à 37 en 2023

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

3

CONFORMITÉ ET CONTRÔLE

516

RÉCLAMATIONS

par rapport à 592 en 2023

Raisons principales :
1. non-respect du droit à l'effacement (18 %) ;
2. non-respect du droit d'accès (17 %) ;
3. confidentialité de données/violation de données (12 %).

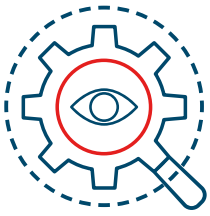
442

NOTIFICATIONS DE VIOLATIONS DE DONNÉES

par rapport à 434 en 2023

Cause principale : erreur humaine (51 %).

Nature des incidents :
1. piratage, hacking (26 %) ;
2. données personnelles envoyées au mauvais destinataire (21 %) ;
3. divulgation de données personnelles de la mauvaise personne (13 %).



29

DOSSIERS D'ENQUÊTES OUVERTS EN 2024

44 dossiers actifs :
- coté **service opération de contrôle** :
  - 27 enquêtes en cours dont 15 ont été ouvertes en 2024
- coté **service analyse des opérations** :
  - 17 dossiers actifs dont 14 ont été ouverts en 2024

UNE ANNÉE EN CHIFFRES

DÉCISIONS

3

DÉCISIONS PRISES PAR LA FORMATION RESTREINTE

- 1 clôturée en l'absence de manquements retenus
- 2 décisions avec mesures correctrices, dont 1 avec amende

2 300 €

D'AMENDES ADMINISTRATIVES

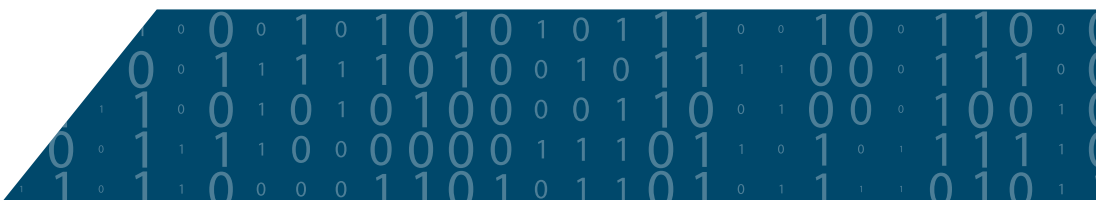
- uniquement dossiers nationaux

RESSOURCES HUMAINES

66

COLLABORATEURS

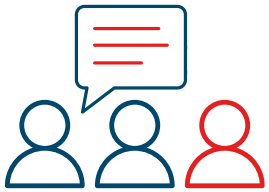
39 ans : moyenne d'âge
5 ans : ancienneté moyenne



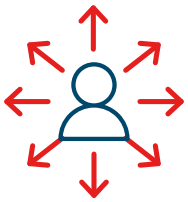
3

EDPB (EUROPEAN DATA PROTECTION BOARD)

152
RÉUNIONS PLÉNIÈRES



126
RÉUNIONS DES GROUPES DE TRAVAIL



35
RÉUNIONS DES TASK-FORCES

LES ACTIVITÉS EN 2024

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.

28 JANVIER 2024 : 18ème 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.

Symposium on Cybersecurity and Data Protection in Humanitarian Action

La CNPD a contribué à l'organisation de la 2e édition du « Symposium on Cybersecurity and Data Protection in Humanitarian Action » (Symposium sur la cybersécurité et la protection des données dans le domaine de l'action humanitaire) du Comité International de la Croix-Rouge, qui a eu lieu du 23 au 25

janvier 2024 dans les locaux du European Convention Center à Luxembourg-ville.

La conférence a réuni des acteurs d'organisations humanitaires, de gouvernements, d'autorités de protection des données, d'agences de cybersécurité, du secteur privé, de la société civile et du monde académique. L'objectif était d'examiner plusieurs défis juridiques, politiques et technologiques soulevés par la transformation numérique de l'action humanitaire.

Tine A. Larsen, présidente de la CNPD, a prononcé un discours lors du symposium, tandis que des représentants de l'autorité de protection des données ont participé à de nombreuses sessions de travail et à des discussions sur ce sujet pertinent en lien avec les activités de la Commission nationale.

La présidente et les commissaires de la CNPD, Marc Lemmer et Alain Herrmann, ont notamment été « chair » et/ou rapporteur pour certaines sessions :

- Data protection, digital risks, data responsibility and ethics: how do these frameworks of analysis interact to guide responsible use of technology in humanitarian action
- The principle of humanity and humanitarian uses for artificial intelligence
- Open-source information and personal data protection

Par ailleurs, des collaborateurs de la CNPD ont participé

- à la Cyberrange, un exercice de groupe qui fait réagir les participants à diverses cybermenaces en tant qu'organisation humanitaire à travers une série de stratégies et tâches techniques et
- au Hackathon, qui a réuni des spécialistes techniques autour de défis spécifiques.

Cet événement a fait partie des activités du DigitHarium, un forum mondial pour discuter et débattre de la transformation numérique dans le secteur humanitaire, en mettant l'accent sur la protection humanitaire, les politiques, l'éthique et l'action.

Le symposium a mis en évidence le fait qu'aujourd'hui, tous les acteurs publics, y compris les organisations humanitaires, doivent assumer leurs responsabilités en matière de protection des données. La numérisation de l'information présente de nombreux risques auxquels il faut faire face, mais aussi des opportunités uniques qui peuvent innover et faciliter le travail humanitaire.

Data Privacy Day avec le thème de l'intelligence artificielle

Le 29 janvier, Maxime Dufour, expert juridique à la CNPD, a donné une présentation sur « L'IA et la protection des données personnelles : comment le RGPD réglemente l'IA et comment l'IA défie le

LES ACTIVITÉS EN 2024

RGPD ». Il s'est penché sur les défis de l'intelligence artificielle en matière de protection des données personnelles à l'ère de l'industrialisation de l'IA, en montrant les conflits potentiels entre la nature de la technologie de l'IA et les principes, obligations et droits découlant du RGPD.

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.

La campagne « Vos données ? Vos droits ! »

Dans le cadre de la Journée de la protection des données, la CNPD a également annoncé le lancement d'une nouvelle campagne de sensibilisation.

Intitulée « Vos données ? Vos droits ! », la campagne explique les droits des citoyens en matière de protection des données personnelles, à commencer par leur droit d'être informés des traitements de données les concernant. Grâce à du matériel d'information adapté aux non-initiés tel qu'une vidéo et une fiche illustrée, le grand public pourra comprendre comment et pourquoi il a le droit de savoir comment ses données personnelles sont collectées et utilisées par les entreprises et autres organismes.

Il s'agissait du premier volet d'une série de publications clarifiant les droits des individus en matière de protection des données d'une manière claire et facilement accessible.

PRIVACY SYMPOSIUM À VENISE

Le Privacy Symposium, une conférence internationale destinée à faciliter le dialogue, la coopération et la convergence parmi experts, chercheurs et autorités de protection des données du monde entier, s'est tenue du 10 au 14 juin à Venise (Italie).

La CNPD a contribué fortement à certaines séances ou éléments du programme de cette conférence qui s'est élevé comme une des rencontres phare de la protection des données au niveau international. Monsieur Alain Herrmann, Commissaire à la CNPD, est intervenu dans plusieurs panels. Monsieur Jérôme Commodi, juriste – gestionnaire de projets à la CNPD, a présenté le projet DAAZ, un outil d'aide à la mise en conformité au RGPD développé par la CNPD en collaboration avec la Luxembourg House of Cybersecurity et le National Cybersecurity Competence Center.

La conférence Privacy Symposium a donné lieu à des échanges fructueux sur les derniers développements et perspectives en matière de protection des données et de la vie privée. Avec plus de 300 autorités et experts partageant leurs perspectives, elle offrait un lieu de rencontre pour les professionnels de la protection des données, les experts, les autorités et les chercheurs promouvant le dialogue international, la coopération et le partage des connaissances sur la protection des données, la conformité et les technologies innovantes.

4

Salon NEXUS2050.

CONFÉRENCE NEXUS2050 : THE INTERNATIONAL TECH PULSE

La CNPD a participé à la première édition de NEXUS2050, le nouveau salon technologique phare au Luxembourg qui sur deux jours réunissait plus de 5000 participants, dont 70 exposants, 300 intervenants et plus de 150 startups les 26 et 27 juin à Luxexpo The Box au Kirchberg.

Sur son stand, la CNPD a présenté ses activités de guidance et de sensibilisation et en particulier les différents outils développés pour faciliter la compréhension et la mise en conformité au RGPD comme la formation Data Protection Basics, les ateliers de travail DaProLab et la certification GDPR-CARPA.

Tine A. Larsen, présidente de la CNPD, a présenté l'outil DAAZ lors d'un intitulé « Re-Skilling and Up-Skilling for today's AI world ». Ensemble avec Alain Herrmann, commissaire à la CNPD, elle a donné un aperçu de la nouvelle plateforme d'apprentissage en ligne de la CNPD, expliquant comment les personnes qui traitent des données personnelles sont sensibilisées sur les obligations et responsabilités qu'elles ont à travers une histoire avec des personnages fictifs, des quiz et d'autres interactions gamifiées.

LES ACTIVITÉS EN 2024

Luxembourg Internet Days 2024.

Sadia Berdaï, juriste à la CNPD, a présenté le bac à sable réglementaire de la CNPD « Sandkëscht », axé sur la protection des données et l'intelligence artificielle. Cet outil permet aux entreprises de tester dans un environnement dédié leurs produit ou service par rapport à la conformité réglementaire relative à la protection des données personnelles et notamment le RGPD.

La CNPD a d'ailleurs pu accueillir à son stand Madame Stéphanie Obertin, ministre de la Digitalisation, accompagnée de ses conseillers au ministère de la Digitalisation et au ministère de la Recherche et de l'Enseignement supérieur ainsi que des représentants du Centre des technologies de l'information de l'État (CTIE) et du Commissariat du Gouvernement à la protection des données auprès de l'État (CGPD).

L'événement a permis aux agents de la CNPD de s'informer sur les tendances et les préoccupations du monde technologique et de nouer des contacts utiles. C'était une opportunité propice de rencontrer et s'échanger avec des acteurs de l'écosystème, notamment des représentants d'entreprises, de start-ups et d'institutions publiques.

LUXEMBOURG INTERNET DAYS 2024

La CNPD était représentée aux Luxembourg Internet Days organisés par LU-CIX les 19 et 20 novembre 2024 dans les locaux de la Chambre de Commerce. La Commission a expliqué ses missions et activités aux participants et a présenté ses initiatives récentes, notamment DAAZ et Sandkëscht. Les agents de la CNPD ont également répondu aux questions et demandes de personnes concernées.

Le premier jour de la conférence, Sadia Berdaï, juriste à la CNPD, a donné une présentation sur l'Open Source Intelligence (OSINT). Elle a expliqué la collecte et l'analyse d'informations accessibles au public et la méthodologie associée avant d'aborder les pratiques commerciales y afférentes. Madame Berdaï a donné un aperçu des obligations découlant du RGPD et clarifié les aspects légaux concernant l'OSINT en termes de protection des données personnelles.

4

Organisés par LU-CIX, les Luxembourg Internet Days (LID) sont un événement de référence pour les discussions et les rencontres au Luxembourg et dans la Grande Région pour les professionnels de l'écosystème de l'Internet et de la cybersécurité. Elles combinent des conférences inspirantes, des tables rondes et des ateliers interactifs, ainsi qu'une exposition. Le LID accueille chaque année plus de 1 100 visiteurs professionnels pour discuter des défis liés à la sécurité de l'Internet, des réseaux et du Cloud, pour explorer les tendances en matière d'attaques et de vulnérabilités cachées.

La connectivité, la sécurité des réseaux et la résilience étaient les thèmes principaux pour aider les opérateurs Internet et les utilisateurs professionnels à rester vigilants et réactifs pour contrer tous les types d'attaques, y compris les attaques DDoS volumétriques ou applicatives les plus innovantes, et obtenir des lignes directrices pour se préparer à la mise en œuvre de la directive NIS2.

FORMATIONS

En 2024, la CNPD a poursuivi ses efforts de sensibilisation à travers des formations et des conférences, permettant de transmettre les messages fondamentaux portés par la commission depuis sa création, tout en les adaptant aux enjeux actuels.

Les initiatives de consolidation des outils pédagogiques, initiées en 2023 avec la formation « Data Protection Basics » (DPB) qui a rencontré un succès notable, ont été renforcées pour permettre une participation élargie. La méthodologie repose sur une approche interactive combinant questions-réponses, quiz et exemples concrets, associés à des explications claires et intuitives des concepts clés. Les retours très positifs des participants témoignent de la pertinence et de l'efficacité de cette démarche pédagogique.

Face à l'apparition massive et globale de l'intelligence artificielle dans notre quotidien le rôle stratégique de la CNPD dans ce domaine au Luxembourg, une nouvelle formation, « Data Protection Basics: Artificial Intelligence » (DPBAI), a été lancée en octobre 2024. Cette initiative vise à fournir aux apprenants une compréhension des concepts fondamentaux, en conciliant les spécificités technologiques de l'IA avec les exigences de protection des données personnelles. À l'instar de la formation « DP-Basics » dans le domaine général de la protection des données, cette nouvelle formation offre des bases solides pour appréhender les enjeux liés à l'IA.

La CNPD a également intensifié ses efforts pour sensibiliser les jeunes en matière de protection des données personnelles. Les cours du BTS professionnel au Lycée Guillaume Kroll à Esch-sur-Alzette ont été mis à jour, et des interventions ont été menées dans d'autres établissements, notamment au Lycée Technique de Bonnevoie, dans le cadre du bachelor en e-commerce, ainsi qu'à Luxembourg, en collaboration avec HEC Liège, pour aborder le thème de l'IA éthique et responsable.

LES ACTIVITÉS EN 2024

En parallèle, les professionnels et parties prenantes ont bénéficié de formations adaptées grâce aux interventions de la CNPD lors de sessions organisées par la Chambre des Salariés, la Chambre de Commerce (House of Training) et la House of Entrepreneurship, entre autres. Ces initiatives témoignent de l'engagement continu de la CNPD à accompagner tous les publics dans la compréhension et l'application des principes fondamentaux de la protection des données.

CONFÉRENCES ET SÉMINAIRES

En plus des conférences organisées par elle-même, la CNPD a aussi participé à des évènements pour sensibiliser aux enjeux de la protection des données.

Le nombre de participations à des conférences dans lesquelles la CNPD était intervenante a augmenté de 29 % par rapport à l'année précédente avec 48 interventions en 2024. Les représentants de la CNPD sont notamment intervenus lors des évènements suivants :

- Conférence « L'intelligence artificielle : aspects juridiques et enjeux pratiques pour les entreprises. », organisée par la Chambre de Commerce dans le cadre du cycle de conférences Ready4AI. La CNPD a apporté des éclaircissements sur l'articulation entre le RGPD et l'IA, et les enjeux pour les entreprises à travers le prisme de la protection des données.

- Conférence « AI Act: impacts for the financial sector? » organisée par l'Association des Banques et Banquiers du Luxembourg (ABBL) et Arendt. La CNPD a donné une présentation intitulée « AI & Protection of personal data: regulation challenges with GDPR and AI Act ».

- Conférence d'Abilways dédiée à la gestion et à la protection des données. La CNPD a présenté les enjeux concernant l'intelligence artificielle et la protection des données, ainsi que le bac à sable règlementaire sur l'intelligence artificielle de la CNPD.

- Table ronde intitulée « Naviguer vers l'Avenir : Mise en Œuvre et Régulation de l'Intelligence Artificielle ».

- Conférence « Regulation of Artificial Intelligence, Internet and Data » (RAID Virtual) sur le thème « Innovate, Regulate and Implement with Courage and Caution ». Participation de la CNPD au panel « Rethinking data Protection ».

- PwC Cybersecurity & Privacy Day, participation à une table ronde sur l'enquête « Out of the shadows: CISOs and DPOs in the spotlight! » et à l'atelier « The latest news from the CNPD » qui a abordé des sujets d'actualité dans le domaine de la protection des données.

- Conférence : « Le Data Act en pratique : partage de données, changement de fournisseur cloud, interopérabilité : comment mettre en œuvre ? ». La CNPD y a participé à la table ronde intitulée « Le Data Act expliqué : Obligations et droits

clés des consommateurs et des entreprises dans le cadre du Data Act : vers une relation transparente et équitable ».

- Assemblée générale de l'APDL (Association pour la protection des données au Luxembourg).
- Bâloise Cybersecurity Day, intervention de la CNPD sur le thème « Sensibiliser nos proches sur les risques Cyber, c'est avoir l'Assurance d'un avenir plus sûr ».
- Conférence RAID (Regulation, AI, Internet, Data), participation de la CNPD à la table ronde « Making Tech Legislation Work in Practice ».
- Conférence « Intelligence Artificielle et Protection des données » organisée par l'APDL. Les présentations de de la CNPD ont porté sur le thème « RGPD et IA: Quels enjeux pour les entreprises ? et sur l'AI Act.
- Healthcare Week Luxembourg 2024, participation à la table ronde « Comment la technologie nous permet d'innover et de créer de la valeur ».
- Session « Ethical & Responsible AI » du cours « Artificial Intelligence » pour les étudiants en MBA à HEC Liège Luxembourg.
- Conférence « Digitalisation in Banking - Driving the Digital Transformation in your Bank » organisée par l'Agence de Transfert de Technologie Financière (ATTF), présentation de la CNPD intitulée « Personal Data Protection: An Introduction to GDPR and an Outlook to the EU Digital Package Regulations ».

12e journée de la protection des données.

- 12e journée de la protection des données, organisée par la Chambre de commerce et d'industrie de Munich et de l'Oberbayern (IHK München und Oberbayern), présentation du bac à sable règlementaire « Sandkëscht ».
- Webinaire organisé par l'association LETZPACT, qui rassemble la communauté des Affaires Publiques au Luxembourg. La CNPD a eu l'occasion d'évoquer ses initiatives récentes en matière de guidance et de sensibilisation.

LES ACTIVITÉS EN 2024

ATELIERS DE TRAVAIL « DAPROLAB »

En 2024, la CNPD a organisé 6 ateliers de travail « DaProLab » pour les acteurs publics et privés de l'écosystème luxembourgeois.

Les ateliers de travail ont porté sur les thèmes suivants :

- L'intelligence artificielle (base légale pour l'entraînement, traitement ultérieur de données, transfert de données vers les pays tiers, transparence et information des personnes concernées) ;
- Le concept de « Privacy by Design » dans le contexte de l'IA ;
- L'IA et la gouvernance des données personnelles au sein des organisations ;
- Les décisions automatisées et plus particulièrement l'article 22 du RGPD ;
- L'Article 32 décrypté, la sécurité des données activée.

Le DaProLab est un atelier collaboratif conçu pour aider les professionnels à adopter une attitude de responsabilisation et à se conformer au RGPD. Il s'agit d'un espace d'échange où les participants partagent leurs idées, interprétations et points de vue sur un sujet spécifique défini à l'avance. Lors de chaque séance, les participants confrontent leurs décisions, prises de position et réflexions avec celles des autres afin d'obtenir un retour constructif sur leurs choix. Cet échange favorise également le partage de connaissances, d'expériences et de bonnes pratiques en matière de protection des données.

La CNPD intervient dans ce cadre en tant que modérateur et médiateur, garantissant un dialogue ouvert et enrichissant entre les participants.

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

Les technologies numériques, la cybersécurité et l'intelligence artificielle font partie des principaux piliers de l'écosystème de l'innovation à Luxembourg. Nombreux sont les acteurs privés et publics qui y sont impliqués et qui réalisent des projets d'innovation digitales.

La CNPD joue un rôle actif dans cet environnement en collaborant plus ou moins activement avec les acteurs afin de favoriser le développement de produits et services respectueux de la protection des données à caractère personnel et de la vie privée.

En 2024, la CNPD a contribué aux projets suivants au niveau de leur comité d'experts :

- DECEPTICON: Projet de recherche interdisciplinaire de l'Université de Luxembourg (SnT/IRiSC) avec le LIST et cofinancé par le FNR (2021 – 2024) pour analyser les designs trompeurs en ligne

pour développer des méthodes et outils de détection de ces formes de manipulation présentes sur internet et dans les médias sociaux.

Ce projet a un intérêt particulier pour la CNPD du fait de la publication par l'EDPB de ses guidelines sur les « deceptive design patterns » pour lesquelles l'Université de Luxembourg a été un important contributeur lors de la phase de consultation publique. Par ailleurs les chercheurs impliqués dans ce projet intervenaient également dans la conférence « Ces cookies nuisent à la vie privée ! » que la CNPD a organisé à l'occasion de l'édition 2022 de la Journée internationale de la protection des données.

- NATIONTWIN : Projet de mise en place d'un centre national d'excellence (NCER) de l'Université de Luxembourg (SnT), le LISER et coordonné par le LIST et soumis fin 2022 dans le programme de financement compétitif NCER du FNR. La proposition a été acceptée début 2025 par le FNR et le projet produire ses premiers délivrables au cours de cette année.

  Le but de ce projet stratégique de dimension nationale est la création du premier prototype de jumeau numérique de confiance à l'échelle d'un pays en se focalisant dans une première approche sur des cas d'usage dans le domaine de l'énergie.

La CNPD apportera son expertise en matière de protection des données personnelles et de la vie privée pour guider les acteurs dans le développement de solutions conformes avec la législation et en appliquant le principe du « Privacy-by-Design ».

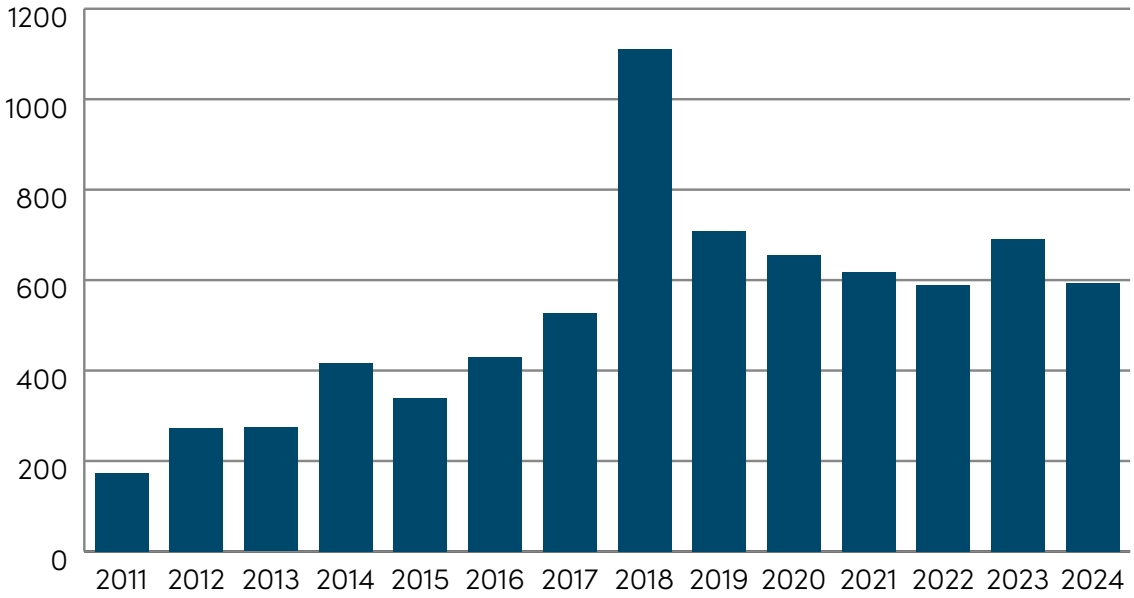
LES ACTIVITÉS EN 2024

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

La CNPD accompagne et informe aussi bien les citoyens que les professionnels. Elle intervient pour apporter des éclaircissements juridiques relatifs aux droits et obligations en matière de protection des données personnelles et guider les acteurs vers la conformité des traitements de données avec la législation en vigueur. Un service dédié est à disposition pour répondre aux demandes d'information reçues par courrier, téléphone ou courriel.

En 2024, 594 demandes d'information écrites ont été traitées, dont 574 demandes nationales et 20 provenant des mécanismes de coopération européenne. Ce chiffre est en baisse par rapport aux 691 sollicitations enregistrées en 2023 (-14 %), mais reste dans la moyenne des cinq dernières années.

ÉVOLUTION DU NOMBRE DE DEMANDES D'INFORMATION PAR ÉCRIT



4

Des entreprises privées ainsi que des autorités publiques ont sollicité la CNPD pour diverses questions concernant la gestion des données personnelles de leurs clients, usagers et employés. Un nombre important de ces demandes concernait la gestion des données dans le cadre des relations de travail, avec une attention particulière accordée aux dispositifs de surveillance instaurés par les employeurs. Ces problématiques incluaient l'utilisation de systèmes de vidéosurveillance sur les lieux de travail, la géolocalisation des véhicules de service et les dispositifs de pointage des employés.

Enfin, la vidéosurveillance, qu'elle concerne des espaces publics ou des propriétés privées, a continué de soulever de nombreuses interrogations, témoignant de l'attention constante du public à ce sujet. Constatant qu'il s'agit d'un sujet récurrent, la CNPD a mis à jour ses lignes directrices en matière de vidéosurveillance, qu'elle a par ailleurs complété d'un modèle pour affichage ainsi que de guidances applicables à des cas particuliers : « la vidéosurveillance dans une copropriété » et « quelle vidéosurveillance dans une habitation privée ? ».

Outre la gestion des données dans le cadre des relations de travail et la vidéosurveillance, les demandes d'informations ont concerné en 2024 notamment les thématiques suivantes :

- les modalités d'exercice du droit d'accès,
- le principe de minimisation des données,
- le consentement au sens du RGPD,
- les modalités d'exercice du droit à l'effacement,
- le droit à l'image,
- la gestion des données liées aux e-mails,
- la gestion des violations de données,
- le rôle de délégué à la protection des données.

La CNPD a reçu également des questions liées au traitement des données dans les secteurs immobilier, financier, public, de la santé, et policier.

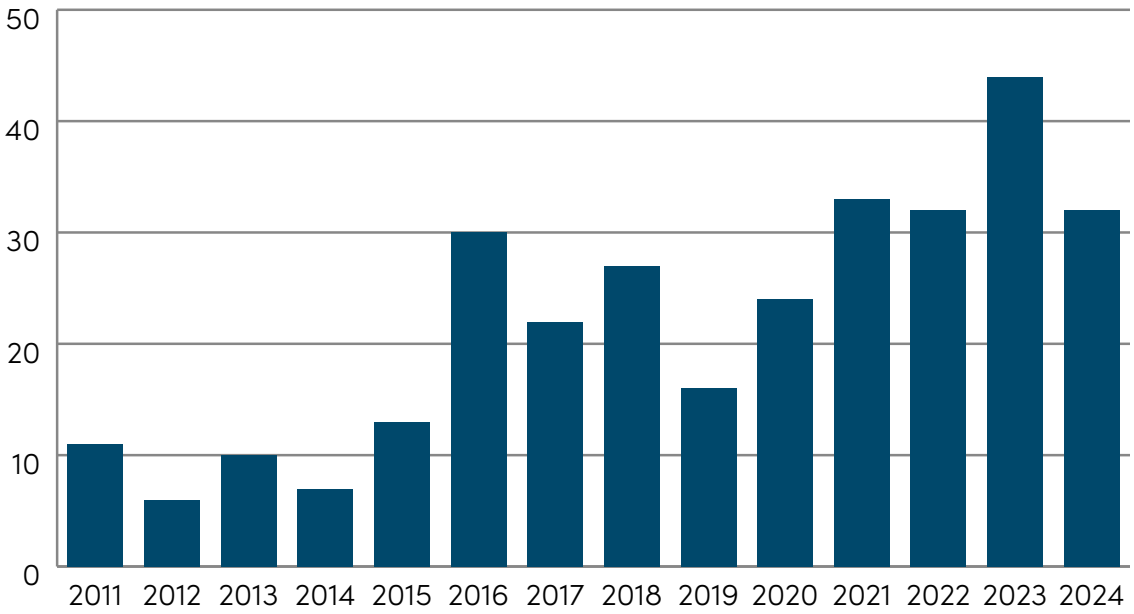
LES ACTIVITÉS EN 2024

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 2024, la Commission nationale a émis 32 avis au total, dont un concernant les traitements de données à caractère personnel en matière pénale, ainsi qu'en matière de sécurité nationale. Cet avis est présenté dans la partie II.2.2) 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.

ÉVOLUTION DU NOMBRE DES AVIS



4

Depuis 2016, on observe une nette hausse du nombre d'avis, une tendance impulsée principalement par les sollicitations accrues du gouvernement et des différents ministères. Ces derniers intègrent désormais de manière croissante des dispositions en matière de protection des données dans les projets de loi ou de règlements grand-ducaux. Par ailleurs, il est à noter que la CNPD a été particulièrement sollicitée lors des périodes de fin de législature de 2018 et 2023, ainsi que durant les phases de préparation et d'implémentation du RGPD (2016 et 2018).

Parmi les avis rendus en 2024, la CNPD voudrait plus particulièrement mettre en avant les avis suivants :

ADMINISTRATION DU CADASTRE ET DE LA TOPOGRAPHIE

En date du 7 août 2024, la Commission nationale a adopté un avis sur le projet de loi n°8330B portant organisation de l'Administration du cadastre et de la topographie et au projet règlement grand-ducal concernant la consultation et la diffusion de la documentation relative à la mensuration officielle, de la documentation cadastrale, de la documentation topographique, du registre national des localités et des rues et des systèmes de référence de coordonnées nationaux gérés par l'Administration du cadastre et de la topographie ; et portant fixation du tarif des redevances 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. Le projet de loi vise à abroger et remplacer la loi du 25 juillet 2002 portant réorganisation de l'administration du cadastre et de la topographie.

Tout d'abord, le projet de loi entend introduire et entériner le principe de « publicité foncière ». La CNPD se demande toutefois s'il ne serait pas opportun de définir ce principe expressément dans la loi. En outre, elle a relevé que la mise à disposition au public par l'Administration du cadastre et de la topographie des données, qui seraient visées par les textes en projet précités, en vertu du principe de « publicité foncière », n'implique aucunement que la réutilisation de telles données par des tiers soit automatiquement licite et légitime au sens des articles 5 et 6 du RGPD, du seul fait que ces données soient considérées comme « publiques ». En effet, sans remettre en question le principe de « publicité foncière », elle estime qu'une vigilance particulière devrait être apportée quant à la licéité des traitements effectués par les professionnels du secteur immobilier à des fins de prospection commerciale. De tels traitements ne seraient licites que si les articles 5 et 6 du RGPD sont respectés.

La CNPD s'est encore félicitée que le projet de règlement grand-ducal limite temporellement la délivrance d'extraits du registre foncier aux destinataires visés par les dispositions en projet. De telles dispositions permettraient ainsi de limiter les abus en ce qui concerne la communication des données. De même qu'elle se félicite que le projet de règlement grand-ducal précise les

LES ACTIVITÉS EN 2024

destinataires auxquels les données seraient communiquées.

Enfin, la Commission nationale a insisté sur le fait qu'il était indispensable que soit mis en place un système d'authentification forte des personnes à l'origine de la demande de délivrance d'un extrait de la documentation cadastrale. En effet, elle a rendu attentif les auteurs du projet de règlement grand-ducal sur l'interprétation de l'article 15. 1. e) du RGPD, qui confère à la personne concernée le droit d'obtenir du responsable du traitement des informations sur les destinataires ou catégories de destinataires auxquels les données personnelles ont été communiquées, suite à l'arrêt de la Cour de justice de l'Union européenne du 12janvier 2023. Or, en l'absence d'un système d'authentification forte des personnes à l'origine de la demande de délivrance d'un extrait du registre foncier, l'ACT ne pourra faire droit à la demande des personnes concernées sur base de l'article 15. 1. e) du RGPD en ce qui concerne les personnes ayant demandé un extrait du registre foncier concernant la propriété des personnes concernées.

RÉTENTION DES DONNÉES

La CNPD a rendu un avis le 16 mai 2024 sur le projet de loi n°8148 relative à la rétention des données à caractère personnel et portant modification : 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État (ci-après le « projet de loi »). Le projet de loi a comme objectif de rendre conforme le cadre légal luxembourgeois en matière de conservation de données à caractère personnel par les opérateurs du secteur des communications électroniques et l'exploitation correspondante des données par les autorités compétentes à la jurisprudence extensive de la Cour de Justice de l'Union européenne.

La conservation des données de trafic et de localisation est une exception au principe de confidentialité des communications consacré par 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 (ci-après la « directive de 2002 »). Ce principe implique que les utilisateurs peuvent s'attendre à ce que tant le contenu de leurs communications que les données de trafic y afférentes restent confidentielles. Le Contrôleur européen de la protection des données définit les données de trafic comme celles : *« traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques. Les données nécessaires pour transmettre la communication varieront selon les moyens de communication utilisés, mais elles comprennent généralement les coordonnées, la date, l'heure et les données de localisation. Bien qu'il convienne de distinguer les données relatives au trafic*

4

des données relatives au contenu, ces deux catégories de données sont très sensibles, puisqu'elles fournissent des informations sur des communications confidentielles (...) ».

La conservation et l'accès à de telles données, ou encore l'interconnexion entre ces différentes catégories de données, représentent une ingérence considérable dans la vie privée des personnes concernées. Afin de protéger la vie privée des utilisateurs, il est dès lors en principe interdit à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés.

Il existe cependant des exceptions à ce principe. L'article 15 de la directive de 2002 permet aux États membres de prévoir des dérogations dans certaines conditions, cet article exige notamment qu'une telle dérogation doit figurer dans un texte législatif et constituer *« une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques (...) »*[1].

Se rendant néanmoins compte de l'utilité des données de trafic pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, le législateur européen a décidé d'amender la directive de 2002 par la directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (ci-après la « directive de 2006 »), obligeant ainsi les États membres à mettre en œuvre une telle dérogation.

L'objectif de la directive de 2006 était d'introduire dans toutes les législations des États membres une dérogation au principe de confidentialité en imposant une conservation obligatoire aux fournisseurs et opérateurs de communications électroniques des données de trafic et de localisation générées ou traitées, afin de les mettre à disposition des autorités compétentes dans le cadre la prévention, la recherche, la détection et la poursuite d'infractions pénales. Cependant, la directive de 2006 n'opérait pas de distinction quant aux personnes dont les données étaient conservées, ni aux catégories de données qui étaient conservées ou aux zones endéans desquelles les données étaient conservées. Ainsi, la conservation qu'elle imposait a été qualifiée de généralisée et

[1] Article 15(1) de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques

LES ACTIVITÉS EN 2024

indifférenciée car elle couvrait la quasi-totalité de la population sur l'intégralité du territoire. De plus, l'accès des autorités compétentes n'était pas délimité, que ce soit par rapport aux personnes disposant d'un accès, aux objectifs justifiant l'accès, à la réutilisation de ces données ou encore à l'existence d'un contrôle préalable. Enfin, la directive prévoyait une durée de conservation générale de 6 mois, sans opérer de distinction par rapport aux catégories de données conservées ou encore par rapport à la finalité pour laquelle elles étaient conservées. Ces raisons ont amené la Cour de Justice de l'Union européenne à annuler la directive de 2006, jugeant que ladite directive ne respectait pas le principe de proportionnalité[2].

Les conséquences de cet arrêt ont varié en fonction des États membres, qui ont eu des difficultés à concilier le principe de proportionnalité avec la conservation des données de trafic et de localisation. Ainsi, la Cour s'est penchée sur cette matière à plusieurs reprises[3], créant ainsi une jurisprudence fournie avec de plus en plus de précisions quant aux exigences qui devraient entourer la rétention des données. Au Luxembourg, il a fallu attendre le dépôt du projet de loi avisé pour voir une tentative de mise en conformité de la législation nationale avec la jurisprudence de la Cour de Justice de l'Union européenne. La CNPD a avisé le projet de loi à la lumière de la jurisprudence de la Cour de Justice de l'Union européenne. À cette fin, elle a comparé chaque mesure de conservation et d'accès envisagée par les auteurs du projet de loi aux exigences de la Cour, y compris en ce qui concerne les durées de conservation choisies. De plus, elle a vérifié si l'encadrement de la conservation proprement dite auprès des opérateurs et fournisseurs de services de communications électroniques répond aux exigences de la Cour. Elle a également pu commenter les propositions de garanties pour les personnes concernées qui accompagnent les différentes mesures envisagées. Enfin, elle a encore saisi l'occasion pour soulever une incohérence concernant ses pouvoirs de supervision des traitements dans le secteur des communications électroniques.

DGA ET LE PRINCIPE « ONCE ONLY »

En date du 20 décembre 2024, la Commission nationale a adopté un

[2] l'arrêt *Digital Rights Ireland et Seitlinger e.a.* rendu le 8 avril 2014

[3] Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970 ;
arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788 ;
arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791 ;
arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790 ;
arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152 ;
arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258 ;
arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702 ;
arrêt du 17 novembre 2022, Spetsializirana prokuratura C-350/21, EU:C:2022:896 ;
arrêt du 30 avril 2024, Procura della Repubblica presso il Tribunale di Bolzano, C-178/22, EU:C:2024:371 ;
arrêt du 30 avril 2024, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370.

4

avis sur le projet de loi n°8395 relatif à 1° la valorisation des données dans un environnement de confiance ; 2° la mise en œuvre du principe « once only » ; 3° la mise en application de certaines dispositions du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) ; 4° la mise en application de certaines dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Le projet de loi vise à introduire en droit luxembourgeois des précisions quant aux traitements de données à caractère personnel effectués par des entités publiques dans le cadre de l'exécution de leurs missions d'intérêts public, ainsi qu'au traitement ultérieur de

LES ACTIVITÉS EN 2024

données à caractère personnel mis en œuvre par lesdites entités publiques. De même, le projet de loi vise à instaurer en droit national l'échange d'informations et de données à caractère personnel entre entités publiques, c'est-à-dire le principe du « once only ».

À titre de remarques liminaires, la Commission nationale a soulevé qu'il serait opportun de scinder le projet de loi en deux projets de loi distincts pour plus de clarté afin de distinguer les dispositions purement nationales, de celles qui visent à implémenter le règlement 2022/868.

Quant aux acteurs désignés par le projet de loi et compétents en matière de traitement ultérieur de données à caractère personnel et d'accès et de réutilisation de données, la CNPD a notamment fait part de ses inquiétudes quant au champ d'application du projet de loi, du fait que celui-ci ne définit pas avec précision les « entités publiques » qui seraient visées par le projet de loi. La Commission nationale a encore relevé le risque potentiel de confusion avec « l'Autorité des données » qui serait créée par le projet de loi avec son autorité.

En ce qui concerne les traitements de données à caractère personnel effectués par les entités publiques dans le cadre de l'exécution de leurs missions d'intérêts public, la CNPD a avisé négativement l'introduction en droit interne d'une telle disposition. En effet, elle estime que cette base légale mènerait indubitablement à créer une insécurité juridique, contrairement à ce qui est avancé par les auteurs du projet de loi qui estiment que cet article aurait pour objet de *« renforcer la sécurité juridique en matière de traitement de données à caractère personnel ».*

En ce qui concerne le système « once only », la Commission nationale s'est interrogée sur la nécessité de prévoir, outre l'État, les administrations et les communes, le mécanisme du « once only » aux établissements publics et des groupements d'intérêts économiques. Elle a notamment encore regretté qu'il ne soit pas précisé dans le texte en projet qu'une entité publique ne peut se procurer des documents contenant des données à caractère personnel qu'auprès des administrations détentrices des données d'origine en cause et non pas auprès d'une entité qui est seulement un destinataire des documents.

Par ailleurs, la Commission nationale a rappelé l'importance de s'assurer que l'information des personnes concernées soit complète et de qualité au regard des exigences posées par l'article 14 du RGPD. De plus, en cas d'exercice du droit d'opposition par la personne concernée, cette information devrait aussi indiquer les modalités alternatives pour effectuer la démarche entreprise sans bénéficier du dispositif du « once only ». La CNPD a encore estimé essentiel qu'une traçabilité précise des échanges soit assurée, permettant l'exercice du droit d'accès sur les données. Cette traçabilité doit permettre de retracer les échanges qui ont eu lieu, entre quelles administrations, à quel moment. À cet égard,

elle recommande la mise en place de moyens techniques qui permettraient à chaque administré de prendre connaissance, de manière simple et consolidée, de l'ensemble des échanges de données le concernant.

En ce qui concerne le traitement ultérieur de données à caractère personnel par les entités publiques, la Commission nationale a notamment relevé que plusieurs textes légaux seraient susceptibles de s'appliquer en sus des dispositions légales du projet de loi. Ainsi, elle s'est interrogée sur l'articulation des textes légaux existants applicables avec les dispositions du projet de loi.

Enfin, en ce qui concerne le volet européen, la CNPD a notamment estimé que ses pouvoirs de contrôle et de sanctions ne se limitent pas à la vérification des conditions reprises dans les autorisations de l'Autorité des données, mais qu'elle serait compétente pour vérifier l'application et le respect de l'intégralité des dispositions du RGPD et de la loi du 1er août 2018.

En ce qui concerne les missions de la Commission nationale en matière de services d'intermédiation de données et d'altruisme des données, elle a relevé qu'il est primordial que le projet de loi délimite précisément le pouvoir normatif de la CNPD en matière de services d'intermédiation de données. Aussi, la CNPD a constaté que des dispositions lui accordant un pouvoir normatif en matière d'enregistrement des organisations altruistes font défaut. Elle estime dès lors nécessaire de compléter le projet de loi en ce sens.

ÉCHANGE DE DONNÉES ÉLECTORALES ENTRE ÉTATS MEMBRES DE L'UE

En date du 8 mars 2024, la Commission nationale s'est prononcée sur le projet de loi n° 8355 portant modification 1° de la loi électorale modifiée du 18 février 2003 et 2° de la loi modifiée du 16 juin 2017 sur l'organisation du Conseil d'État, qui a pour objet de simplifier les procédures d'échange de données électorales entre les États membres de l'Union européenne afin d'éviter le double vote lors des élections européennes.

Dans son avis, la CNPD a tout d'abord rappelé la nécessité de respecter le principe de minimisation des données prévu par le RGPD. En effet, le projet de loi confie au Centre des technologies de l'information de l'État (le « CTIE ») la mission d'établir une liste contenant les données des électeurs européens inscrits au Luxembourg. Cette liste est ensuite transmise au Ministre ayant les Affaires étrangères dans ses attributions, qui informe les autorités des États membres d'origine respectifs des électeurs inscrits. La CNPD a souligné que cette liste, établie par le CTIE, devrait se limiter aux seules données nécessaires eu égard des finalités pour lesquelles elles sont traitées.

De plus, la Commission nationale s'est interrogée sur la question de savoir qui est effectivement compétent pour transmettre la liste contenant les données électorales aux autres États membres et si une responsabilité conjointe pourrait exister. À cet égard, elle

LES ACTIVITÉS EN 2024

a souligné que les dispositions du projet de loi devraient refléter la réalité des activités exercées par les différents acteurs et donner des indications suffisamment claires permettant d'identifier l'entité qui est à considérer comme responsable du traitement.

Par ailleurs, la CNPD a salué plusieurs dispositions contribuant au respect du principe de minimisation des données consacré à l'article 5. 1. c) du RGPD. Le projet de loi prévoit notamment la suppression de l'envoi de listes contenant des données sensibles des électeurs sous tutelle et l'abandon de l'obligation de renseigner la profession des présentants figurant sur les listes lors du dépôt.

Finalement, la CNPD a constaté que les informations à renseigner sur les listes des candidats lors du dépôt varient selon qu'il s'agit des élections législatives, communales ou européennes. Elle a invité les auteurs du projet de loi à reconsidérer, pour chaque donnée personnelle, la nécessité de la faire figurer dans les listes électorales afin de garantir la conformité aux principes du RGPD.

FICHES D'HÉBERGEMENT

Le projet de loi n° 8253 relative aux fiches d'hébergement et portant: 1° modification de loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 2° modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ; et 3° abrogation de la loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement (le « projet de loi »), vise à remplacer la loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement, qui impose aux exploitants d'un établissement d'hébergement d'établir des fiches reprenant des informations relatives aux personnes hébergées et de les transmettre à certaines autorités à des fins sécuritaires et statistiques[4]. En effet, le Luxembourg est tenu en vertu de la Convention d'application de l'Accord de Schengen de prendre des mesures pour assurer que les étrangers, qui sont hébergés dans un établissement d'hébergement touristique, remplissent et signent une fiche de déclaration et justifient de leur identité. En outre, le Luxembourg doit fournir à l'office statistique de la Commission européenne (EUROSTAT) des statistiques sur la fréquentation des établissements d'hébergement.

Dans son avis initial du 29 mars 2024, la Commission nationale a notamment salué que le projet de loi prévoit une réduction de la durée de conservation des fiches d'hébergement auprès des exploitants[5]

[4] La Police grand-ducale, le Service de renseignement de l'État, et l'Institut national de la statistique et des études économiques du Grand-Duché de Luxembourg.

[5] Article 1er, 1° du projet de loi dispose que l'exploitant est *« toute personne physique ou morale désignée comme exploitant sur la fiche d'hébergement qui fournit à titre onéreux un service d'hébergement touristique ».*

et a rappelé qu'en vertu du principe de limitation de la conservation, les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées ou traitées. Cependant, la Commission nationale s'est interrogée sur la nécessité de la transmission automatique et généralisée des données à la Police grand-ducale. Elle s'est ainsi ralliée aux observations du Conseil d'État selon lesquelles une transmission systématique et généralisée des fiches d'hébergement de l'ensemble des voyageurs qui sont hébergés sur le territoire du Grand-Duché à la Police grand-ducale constitue une ingérence disproportionnée au droit à la protection de la vie privée et au droit à la protection des données à caractère personnel des personnes concernées.

Dans son avis complémentaire du 6 décembre 2024, la Commission nationale a estimé que les amendements parlementaires prévoyant la création d'un fichier des fiches d'hébergement, tenu par le Ministre ayant le Tourisme dans ses attributions (le « ministre »), accessible à la Police grand-ducale et au SRE, demeure une ingérence disproportionnée au regard du droit à la vie privée et à la protection des données. Bien que les amendements parlementaires prévoient un encadrement de l'accès de la Police grand-ducale et du SRE aux données des voyageurs, la CNPD a exprimé ses inquiétudes quant la conformité de ces dispositions avec la jurisprudence de la Cour de justice de l'Union européenne.

En outre, la CNPD s'est notamment interrogée sur le contrôle effectif du ministre concernant la gestion du fichier et si le ministre a la possibilité d'accéder aux données contenues dans ce fichier, estimant qu'un tel accès serait difficilement conciliable avec les principes fondamentaux du droit à la protection des données à caractère personnel. Enfin, la Commission nationale s'est particulièrement interrogée sur les raisons pour lesquelles le ministre se verrait confier cette mission et a regretté que les auteurs des amendements parlementaires n'aient pas précisé les motifs justifiant ce choix.

VIDÉOSURVEILLANCE DANS LES TRANSPORTS PUBLICS

La CNPD a adopté un avis en date du 2 mai 2024 sur le projet de loi n° 8335 relative à la sécurité, la sûreté, l'ordre et la vidéosurveillance dans les transports publics et modifiant la loi du 5 février 2021 sur les transports publics. Le projet de loi a pour objet d'établir de nouvelles normes visant à garantir l'ordre et à renforcer la sécurité dans les transports publics. Il prévoit notamment l'installation de caméras de surveillance à des points stratégiques afin de contribuer à la prévention des infractions et d'assurer la sécurité des personnes et la protection des biens.

Tout d'abord, la CNPD s'est interrogée sur les traitements de données à caractère personnel que les agents de service des transports publics sont, le cas échéant, amenés à mettre en œuvre. En effet, le projet

LES ACTIVITÉS EN 2024

de loi prévoit que lesdits agents, une fois agréés par le ministre ayant les Transports dans ses attributions, peuvent collecter certaines données personnelles des usagers ayant commis des infractions. À cet égard, la CNPD a recommandé de clarifier qui est à qualifier responsable du traitement de données à caractère personnel mis en œuvre par les agents de service agréés lorsqu'ils procèdent à des constats d'infractions.

La CNPD s'est également interrogée sur la manière dont le respect des injonctions de quitter les transports publics, notamment en cas de violation potentielle de ladite injonction, pourrait être prouvé sans trace écrite, et a relevé que des précisions devraient être insérées dans le texte de loi en projet, étant donné que cela pourrait impliquer un traitement supplémentaire de données personnelles.

De plus, la CNPD s'est félicitée que le projet de loi vise à conférer une base légale aux traitements de données effectués dans le cadre de la mise en place des caméras à bord et à l'extérieur des moyens de transport public ainsi que dans les infrastructures de transports publics. La Commission a cependant estimé qu'il est essentiel de prévoir dans le texte du projet de loi des critères objectifs encadrant la mise en place des caméras de surveillance afin d'éviter toute collecte disproportionnée de données à caractère personnel. Elle a recommandé d'exclure explicitement le recours à des techniques de reconnaissance faciale.

En ce qui concerne les modalités d'information des personnes concernées, la CNPD a recommandé d'adopter une approche d'information en deux niveaux et a renvoyé à ses lignes directrices en matière de vidéosurveillance. En outre, la CNPD s'est interrogée sur la manière dont les usagers pourraient être informés, en temps utile, de la présence d'éventuelles « dashcams » installées à l'extérieur des moyens de transports publics.

Concernant la durée de conservation des images, la CNPD a estimé que la période de six mois, prévue par le projet de loi, semble disproportionnée au regard des finalités poursuivies. Elle a recommandé de réduire cette durée, en tenant compte du fait que les réglementations française et belge relatives aux caméras susceptibles de capturer des images de la voie publique limitent généralement la conservation des images à un mois.

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.

4

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 des publics spécifiques identifiés comme étant prioritaires.

En 2024, la CNPD a créé ou mis à jour de nombreux dossiers, dont notamment ceux mentionnés ci-dessous.

MISE A JOUR DES LIGNES DIRECTRICES SUR LA VIDEOSURVEILLANCE

Les caméras sont aujourd'hui largement utilisées tant dans l'espace public que privé. Si ces outils sont légitimes pour assurer la sécurité des biens et des personnes, ils ne peuvent pas conduire à placer les particuliers sous surveillance à n'importe quel moment et à n'importe quel endroit.

Afin de faciliter la compréhension de ce sujet pertinent, la CNPD a publié en 2018 des lignes directrices en matière de vidéosurveillance qu'elle a mis à jour en 2024. Cette actualisation tient en particulier compte des décisions rendues par la CNPD sur le sujet au cours des dernières années ainsi que des lignes directrices émises par l'EDPB.

La CNPD a notamment apporté des précisions quant aux finalités qui pourraient motiver l'installation d'une vidéosurveillance, quant à la forme et le contenu de l'information à fournir aux personnes visées par la vidéosurveillance, et par rapport aux cas spécifiques que sont la vidéosurveillance dans les copropriétés et le recours à des caméras factices.
Elle rappelle en particulier que toute personne susceptible d'entrer dans le champ de vision des caméras de vidéosurveillance doit être informée de la présence de celles-ci. Afin de faciliter la compréhension des personnes filmées, la CNPD a suggéré de mettre en place une information à deux niveaux : un premier niveau avec la communication des informations les plus importantes via un panneau d'affichage bien visible, renvoyant vers un deuxième niveau qui fournit l'ensemble des informations obligatoires.

Cette mise à jour, contient également une proposition de modèle pour afficher l'information du premier niveau à adapter au cas par cas.

MISE À JOUR DES LIGNES DIRECTRICES SUR LES CAMPAGNES ÉLECTORALES

En prévision des élections européennes du 9 juin 2024 au Luxembourg, la CNPD a rappelé les règles à respecter concernant

LES ACTIVITÉS EN 2024

la protection des données à caractère personnel, détaillées dans ses lignes directrices actualisées.

Parmi les autres aspects abordés dans les lignes directrices, il y a lieu de citer, de manière non exhaustive, le traitement de données sensibles, la provenance des données personnelles, la prospection politique et le ciblage.

GARANTIR LA RÉSILIENCE CONTRE LES ATTAQUES INFORMATIQUES

Au Grand-Duché, la protection des données a été au cœur des préoccupations en 2024 suite à une attaque DDOS d'envergure qui a paralysé plusieurs sites gouvernementaux, entraînant une indisponibilité des données. Cette attaque souligne la vulnérabilité des systèmes informatiques face aux cybercriminels qui cherchent à exploiter toute faille pour accéder à des données personnelles sensibles.

Dans ce contexte, la CNPD a publié un article qui présente plusieurs bonnes pratiques en protection des données pour renforcer la cybersécurité.

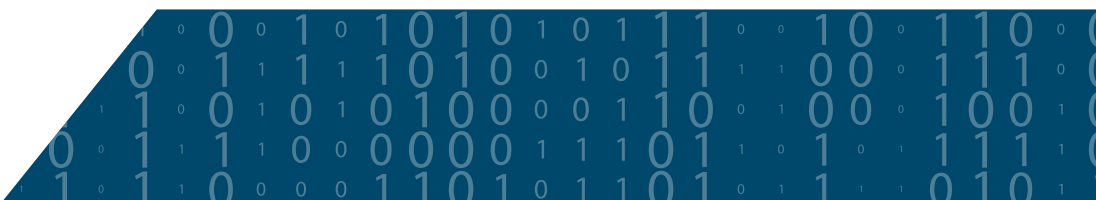
RECOMMANDATIONS RELATIVES À LA TRANSPARENCE DANS LE SECTEUR DES SERVICES EN LIGNE

La CNPD a publié un rapport d'information sur les enquêtes relatives à la transparence dans le secteur des services en ligne menées entre 2020 et 2022.

La transparence n'est pas une notion nouvelle mais une caractéristique bien ancrée en matière de protection des données. Elle prend un sens d'autant plus important dans le domaine des services en ligne, compte tenu des spécificités de ce secteur et du fait que l'intégralité des interactions sont opérées de manière virtuelle. En outre, des lignes directrices claires relatives à la transparence ont été définies par l'EDPB et sont disponibles depuis novembre 2017. L'objectif premier de la transparence est l'installation de la confiance entre les responsables du traitement et les personnes concernées. La notion de transparence prend une dimension encore plus forte avec le RGPD et le principe d'accountability, auquel elle est intrinsèquement liée. La transparence permet aux personnes concernées de savoir ce que le responsable de traitement fait de leurs données personnelles et d'exiger des responsables du traitement qu'ils rendent des comptes à cet égard.

Conformément à l'article 58 du RGPD, la CNPD a le pouvoir de lancer des enquêtes de sa propre initiative. Ces enquêtes dites « proactives » peuvent être effectuées sous forme d'enquêtes thématiques portant sur les obligations du RGPD auprès de différentes organisations.

Entre 2020 et 2022, la CNPD a mené des enquêtes thématiques sur la transparence dans le secteur des services en ligne portant sur 6 organismes établis au Luxembourg et proposant des services en ligne dans différents domaines



(commerce, restauration, loisirs et autres services). Ce choix a été motivé notamment par la forte croissance qu'ont connu certains services en ligne dans le cadre de la pandémie.

Pour réaliser ces enquêtes, le chef d'enquête s'est notamment basé sur les documents d'orientations générales fournis par l'EDPB. L'objectif de ces enquêtes thématiques était de s'assurer que les responsables du traitement qui collectent des données auprès des personnes concernées le font dans le respect des articles 12 point 1, 13 et 14 du RGPD.

Le rapport d'information constitue une synthèse publique des travaux et des résultats de ces enquêtes. La première partie présente les objectifs et le déroulement des travaux d'enquête. La seconde partie présente les résultats des travaux d'enquête. La troisième partie décrit les décisions prises par la formation restreinte relatives à ces enquêtes. Enfin, la quatrième partie présente les recommandations de la CNPD relatives à la transparence.

PREMIERS RETOURS D'EXPÉRIENCE SUR LA PROTECTION DES DONNÉES, NUMÉRISATION ET INNOVATION AU LUXEMBOURG

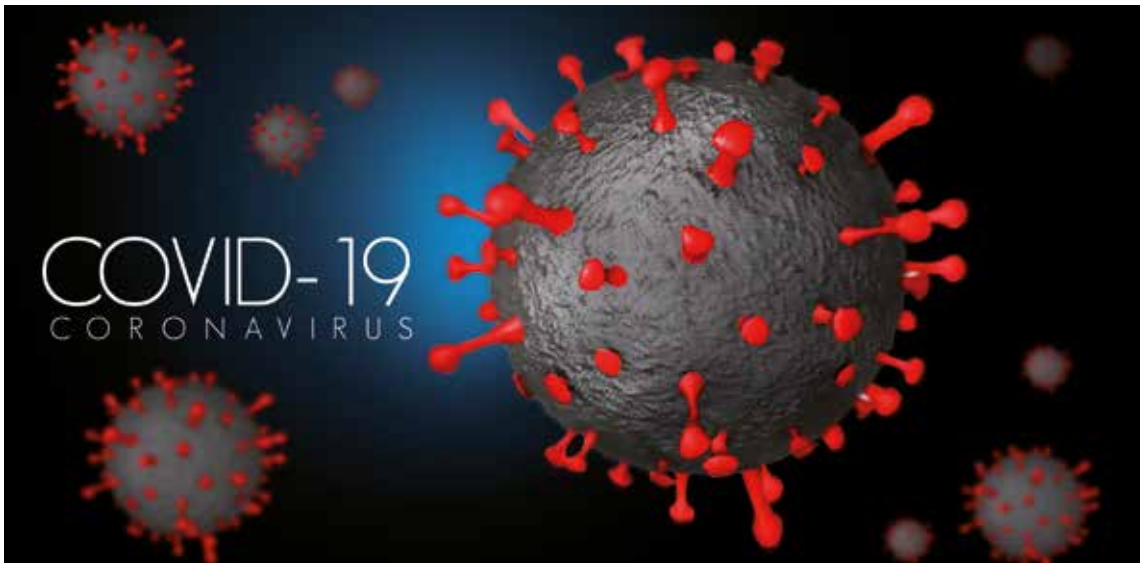
La CNPD s'engage activement à promouvoir une économie responsable et respectueuse de la protection des données à caractère personnel et de la vie privée. C'est dans cette optique que la Commission a lancé en janvier 2024 un appel à contribution visant à mieux comprendre les problématiques des acteurs de l'écosystème luxembourgeois par rapport à la protection des données à caractère personnel, notamment vis-à-vis de l'utilisation de l'intelligence artificielle.

Dans un article, la CNPD reprend les points principaux soulevés par l'appel à contributions et présente les mesures qu'elle a proposé, conformément à sa mission de guidance.

COMPRENDRE LES VIOLATIONS DE DONNÉES POUR MIEUX PROTÉGER LES DROITS ET LIBERTÉS DES PERSONNES ET ACCOMPAGNER LES RESPONSABLES DE TRAITEMENT

Alors que l'année 2024 a marqué le sixième anniversaire de l'entrée en application du RGPD en Europe, il était temps de faire un bilan des enseignements tirés des notifications de violations de données à caractère personnel au Luxembourg. Dans un article à ce sujet, la CNPD a donné un aperçu qualitatif et quantitatif sur les informations récoltées au cours de ces années.

LES ACTIVITÉS EN 2024



OBSERVATIONS SUR LES TRAITEMENTS DES DONNÉES RÉALISÉES DANS LE CONTEXTE DE LA PANDÉMIE COVID-19

En 2024, la CNPD a complété son dossier thématique sur le Covid-19 avec un bilan de ses activités de surveillance dans le contexte de la pandémie.

Le document se concentre sur les observations faites par la CNPD dans le cadre du système d'information spécifiquement mis en place à l'époque pour lutter contre la pandémie, ainsi que les nouveaux traitements de données réalisés par les organisations publiques et privées luxembourgeoises pour s'adapter à la situation exceptionnelle.

4

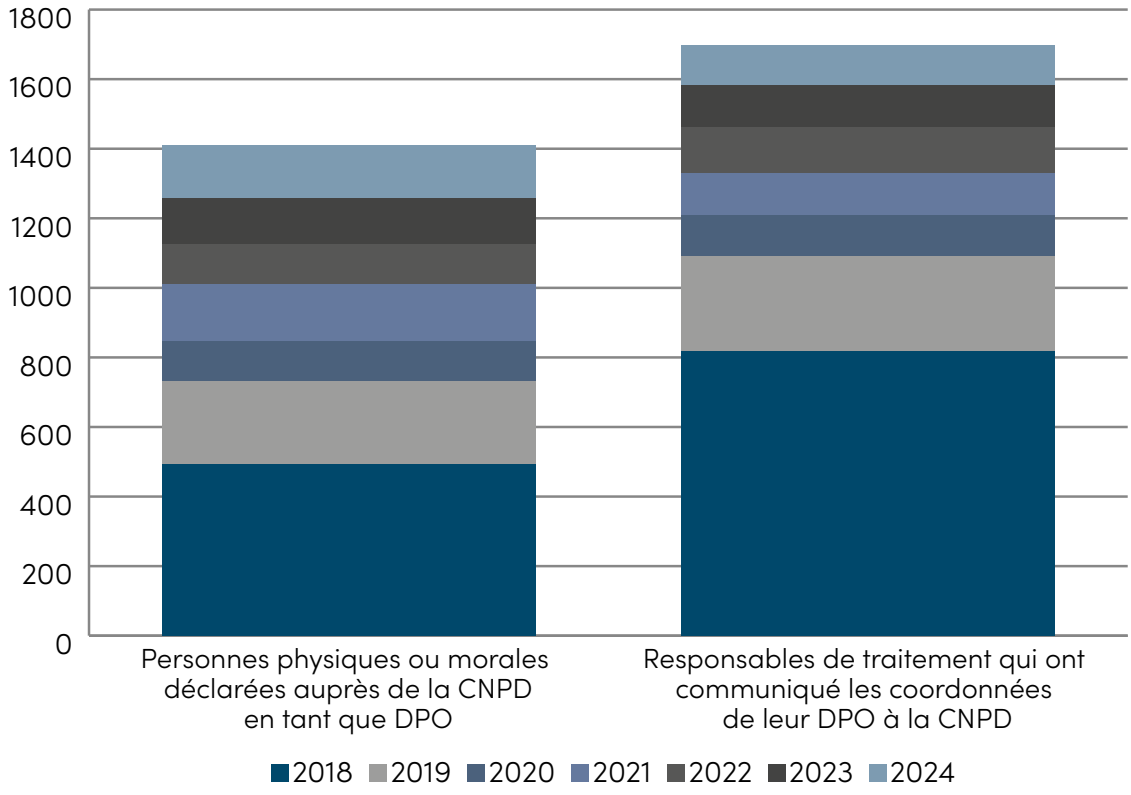
5 DÉSIGNATION DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES

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 2024, 113 responsables du traitement ont communiqué les coordonnées de leur DPD à la Commission nationale. Depuis la date d'entrée en application du RGPD, le 25 mai 2018, 1 696 responsables du traitement ont effectué cette démarche.

Au total, 1 441 personnes physiques ou morales ont été déclarées auprès de la CNPD, dont 154 en 2024.

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.



LES ACTIVITÉS EN 2024

À 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.

À moins qu'il soit 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.

4

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.

RÉORGANISATION INTERNE ET CRÉATION DU SERVICE « IA, INNOVATION ET NUMÉRIQUE »

Pour répondre à l'évolution rapide des défis technologiques et règlementaires, la CNPD a entrepris une réorganisation interne significative en transformant le service « Outil de Support et Innovation » en service « IA, Innovation et Numérique ». Cette nouvelle structure vise à renforcer l'accompagnement des projets d'innovation, en mettant un accent particulier sur l'intelligence artificielle et la protection des données. Le service se prépare également à assumer de nouvelles missions en lien avec la mise en œuvre du règlement européen AI Act.

Règlement de l'UE concernant l'intelligence artificielle

Le 12 juillet 2024, le règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées relatives à l'intelligence artificielle a été publié au Journal officiel de l'UE.

Le règlement de l'UE concernant l'IA (« AI Act ») est le tout premier acte législatif au monde en matière d'IA. L'objectif des nouvelles règles est de promouvoir une IA digne de confiance en Europe et au-delà, en veillant à ce que les systèmes d'IA, tout en ouvrant la voie à une multitude d'application innovantes, respectent les droits fondamentaux, la sécurité et les principes éthiques et en s'attaquant aux risques liés à des modèles d'IA très puissants et percutants.

En décembre 2023, le Parlement européen et le Conseil de l'UE sont parvenus à un accord politique sur la loi sur l'IA. La loi sur l'IA est entrée en vigueur 20 jours après sa publication au Journal officiel et sera pleinement applicable deux ans plus tard soit début 2026, à quelques exceptions près : les interdictions entreront en vigueur après six mois, les règles de gouvernance et les obligations relatives aux modèles d'IA à usage général deviendront applicables après 12 mois et les règles applicables aux systèmes d'IA - intégrés dans des produits réglementés - s'appliqueront après 36 mois. Afin de faciliter la transition vers le nouveau cadre réglementaire, la Commission européenne a lancé le pacte sur l'IA, une initiative volontaire qui vise à soutenir la mise en œuvre future et invite les développeurs d'IA d'Europe et d'ailleurs à se conformer à l'avance aux principales obligations de la loi sur l'IA.

Axé fortement sur l'innovation, l'AI Act vise à établir un équilibre entre l'objectif

LES ACTIVITÉS EN 2024

d'encourager l'esprit d'entreprise et l'obligation de protéger les droits des citoyens. Ce règlement impactera sans doute les compétences de la CNPD et nécessitera une coopération accrue entre la Commission nationale et différents régulateurs, tant au niveau national qu'européen. Dans le cadre de ce texte, la CNPD reste compétente afin de surveiller les éventuels traitements de données à caractère personnel mis en œuvre par les divers acteurs.

DaProLab Reloaded

La CNPD a relancé ses ateliers de travail DaProLab par une série d'évènements ayant permis d'aborder des problématiques émergentes liées à la protection des données dans un contexte d'innovation rapide, notamment :

- Les enjeux de l'intelligence artificielle (IA) et leurs implications éthiques et juridiques.
- Les défis concrets rencontrés par les innovateurs pour se conformer aux exigences du RGPD.

Ces discussions ont réuni divers acteurs de l'écosystème technologique et règlementaire, favorisant une compréhension mutuelle et la recherche de solutions pratiques.
Le DaProLab est un forum de discussion, organisé et modéré par la CNPD. Il s'agit de séances d'échanges d'idées et de points de vue sur des sujets spécifiques entre professionnels de la protection des données. Les participants peuvent confronter leurs analyses et décisions et obtenir des retours d'expérience, ce qui favorise l'échange de connaissances et d'expériences, et, in fine, fait croître la maturité des participants par rapport à l'application du RGPD dans le contexte de l'IA.

Lancement de l'initiative Sandkëscht

Dans le cadre de son engagement à soutenir l'innovation responsable, la CNPD a mis en place un bac à sable règlementaire dénommé « Sandkëscht ». Cet espace contrôlé offre aux innovateurs une opportunité unique de tester leurs projets par rapport à leur conformité au RGPD. L'initiative permet également d'identifier des points d'amélioration d'un point de vue de la protection des données dans la conception des projets technologiques avant leur mise en production. En favorisant une collaboration proactive entre régulateurs et innovateurs, le bac à sable de la CNPD vise à réduire les risques règlementaires et à accélérer l'adoption de bonnes pratiques en matière de protection des données.

4

Renforcement et élargissement des actions de sensibilisation et de formation

Dans le cadre de la sensibilisation aux enjeux de la protection des données et des nouvelles technologies, notamment les systèmes d'intelligence artificielle, le service IA, Innovation et Numérique de la CNPD a commencé en 2024 à développer des supports pédagogiques en collaboration avec le Digital Learning Hub (DLH). Des guides pratiques et des supports de vulgarisation sont en cours de développement pour expliquer les enjeux de l'intelligence artificielle et de la protection des données. Ces ressources seront utilisées lors de formations proposées par la CNPD au cours de l'année 2025.

La CNPD a également développé une formation intitulée « Data Protection Basics: Artificial Intelligence », qui a rencontré un grand succès. Cette formation vise à comprendre les défis de l'intelligence artificielle dans un contexte de protection des données et vie privée et de RGPD. Elle s'adresse à ceux ayant déjà de bonnes connaissances en protection des données. Les thèmes abordés incluent les aspects techniques de l'IA, la gestion des données et les liens entre le RGPD et l'AI Act. Cette formation continue d'être dispensée en 2025.

Conclusion : une année tournée vers l'innovation responsable

En 2024, la CNPD a encore une fois démontré et renforcé son engagement à accompagner l'innovation dans le respect des droits fondamentaux. Avec le soutien du nouveau service « IA, Innovation et Numérique », la CNPD se positionne comme une autorité soutenant l'écosystème technologique luxembourgeois, en favorisant une innovation respectueuse des législations sur la protection des données et de la vie privée et en anticipant les défis liés à l'intelligence artificielle. Les initiatives mises en place cette année constituent une base solide pour poursuivre cet engagement dans les années à venir.

LES ACTIVITÉS EN 2024

INTERVIEW

SADIA BERDAÏ
Chef de service IA,
Innovation et Numérique

En mai 2024, la CNPD a lancé l'initiative Sandkëscht, un bac à sable réglementaire axé sur le RGPD et les nouveaux usages des données. C'est une première au Luxembourg visant à soutenir les organisations luxembourgeoises (organismes publics ou privés, grandes entreprises, PME ou start-ups) dans un cadre sécurisé et contrôlé. Dans un contexte européen en évolution rapide, avec l'arrivée de l'IA Act, la CNPD a entamé une réflexion et des travaux pour adapter ses missions et ses outils. Sadia Berdaï, Responsable du service IA, Innovation et Numérique, revient sur cette année significative.

4

MADAME BERDAÏ, 2024 A ÉTÉ UNE ANNÉE IMPORTANTE POUR VOTRE SERVICE. COMMENT LA RÉSUMERIEZ-VOUS EN QUELQUES MOTS ?

2024 a été avant tout une année de préparation stratégique. Nous avons pris le temps de partir de nos hypothèses, de clarifier nos ambitions et d'identifier les besoins des acteurs luxembourgeois en matière d'innovation, d'intégration des outils technologiques et d'adaptation des fonctions de support aux nouveaux usages de la donnée. Ce travail de fond était indispensable pour anticiper les futures missions de la CNPD dans le cadre des nouveaux règlements européens, notamment l'AI Act.

PARLONS DE SANDKËSCHT, LE BAC À SABLE RÉGLEMENTAIRE LANCÉ EN MAI. QUELS ONT ÉTÉ LES PREMIERS RETOURS ET ENSEIGNEMENTS DE CETTE INITIATIVE ?

Nous avons reçu un excellent accueil de la part des parties prenantes, des entreprises, des organisations professionnelles des décideurs dans l'écosystème. Sandkëscht a permis de créer un espace de dialogue et d'expérimentation sécurisé, où les acteurs peuvent tester des projets innovants tout en intégrant les exigences du RGPD dès la conception. C'est aussi un outil précieux pour la CNPD, car il nous donne une visibilité sur les nouveaux usages de la donnée et nous permet d'ajuster nos recommandations en fonction de cas concrets.

Cette première itération fournit déjà de nombreux apprentissages. Le dialogue avec les acteurs a permis d'obtenir un retour sur leur perception de la CNPD en tant que régulateur. Les différents échanges ont permis de comprendre les considérations des start-ups et les défis opérationnels liés à la participation à une initiative comme un bac à sable réglementaire, notamment lorsque les ressources humaines sont limitées et souvent multi-tâches, avec des collaborateurs impliqués dans la production, la promotion et la vente de leurs produits ou services. Les grandes entreprises, elles, ont fait part des considérations relatives aux chaînes de décision plus complexes.

En outre, nous avons observé que certains concepts, initialement perçus comme acquis, se révèlent plus abstraits et complexes en pratique. En effet, le champ d'action du bac à sable réglementaire dépasse les départements informatiques ou juridiques, intégrant également des fonctions de support qui expriment des besoins relatifs à l'évolution de leurs métiers et de leurs rôles dans un contexte de transformation numérique et d'intégration d'outils d'intelligence artificielle.

EN QUOI CETTE INITIATIVE S'INSCRIT-ELLE DANS LA STRATÉGIE DE LA CNPD FACE AUX NOUVEAUX RÈGLEMENTS EUROPÉENS COMME L'AI ACT ?

Sandkëscht est une première réponse concrète à notre volonté d'être un facilitateur et un partenaire de confiance pour les acteurs luxembourgeois. L'AI Act va introduire de nouvelles obligations et responsabilités. Nous devons donc anticiper et créer des dispositifs pour accompagner ces acteurs

LES ACTIVITÉS EN 2024

dans cette transition. En 2024, nous avons lancé un projet structurant pour évaluer les ressources, compétences et outils dont nous aurons besoin en cas de nouvelles attributions.

QUELS SONT LES BESOINS QUE VOUS AVEZ IDENTIFIÉS CHEZ LES ACTEURS LUXEMBOURGEOIS DANS CE CONTEXTE ?

Les entreprises, start-ups et fonctions support nous ont exprimé le besoin d'avoir des référentiels pratiques, des guidelines adaptées aux cas d'usage et un accompagnement pédagogique pour appréhender les exigences du futur cadre réglementaire.

Un autre point essentiel qui ressort de nos échanges, c'est la demande de vulgarisation des concepts juridiques et réglementaires. Toutes les entreprises ne disposent pas forcément en interne des compétences spécialisées pour décrypter ces textes parfois complexes. Et du côté des start-ups, les moyens limités rendent souvent difficile le recours à des conseils professionnels externes.

Les acteurs luxembourgeois attendent donc du régulateur qu'il joue aussi un rôle de pédagogue et de facilitateur, en rendant les textes accessibles et opérationnels. Ils cherchent un interlocuteur capable de les conseiller en amont des projets innovants et de les aider à intégrer les exigences de conformité tout au long de leur transformation numérique.

QUELS SERONT LES PROCHAINS JALONS POUR VOTRE SERVICE EN 2025 ?

L'année 2025 sera consacrée à la coopération, ainsi qu'à la mise en œuvre et au déploiement des dispositifs élaborés durant l'année 2024. Nous continuerons à structurer Sandkëscht, à renforcer notre expertise en intelligence artificielle, et à proposer de nouveaux formats d'échange avec les acteurs luxembourgeois.

L'objectif est de se préparer et de s'équiper pour répondre aux nouvelles exigences européennes en matière de données et d'intelligence artificielle.

4

LANCEMENT OFFICIEL DE DAAZ (« DATA ACCOUNTABILITY FROM A TO ZEN »)

Data Accountability from A to Zen

L'outil DAAZ, acronyme de « Data Accountability from A to Zen », est une initiative de la CNPD, en collaboration avec la Luxembourg House of Cybersecurity et le National Cybersecurity Competence Center (LHC-NC3). Cet outil a été conçu pour aider les start-ups et les petites et moyennes entreprises (PME) à se conformer au Règlement général sur la protection des données (RGPD) de manière « fun », intuitive et gratuite.

DAAZ a pour objectif principal de fournir aux acteurs un moyen efficace d'intégrer leurs obligations en matière de protection des données dans leurs activités quotidiennes. En utilisant des méthodes de « story learning » et de « learning by doing », DAAZ vise à rendre la protection des données accessible et compréhensible, même pour ceux qui ne sont pas experts en la matière.

Sélectionné dans un appel à projet compétitif de la Commission européenne, DAAZ a été cofinancé par l'Union européenne dans le cadre du projet ALTO (« dAta Protection compLiance supporT tOolkit »).

Le projet ALTO s'est déroulé en deux phases distinctes réparties sur 20 mois. La première phase a consisté à identifier les besoins spécifiques des PME en matière de protection des données. Pour ce faire, la CNPD a recueilli les avis de 215 entrepreneurs via un questionnaire en ligne. La CNPD a souhaité dès la phase initiale de centrer l'outil sur l'expérience utilisateur, afin de s'assurer que l'outil à développer réponde effectivement aux attentes et aux défis rencontrés par les PME.

La deuxième phase a impliqué le développement technique et pédagogique de l'outil, avec l'aide précieuse des développeurs du LHC-NC3 et d'un UX designer. Lors de la phase de développement, la CNPD a décidé de mettre en oeuvre les concepts de narration et d'immersion, combinée au concept de gamification, afin de maximiser l'engagement des utilisateurs et faciliter leur apprentissage. Cette phase a également inclus des tests avec des PME volontaires pour optimiser l'outil et garantir son efficacité.

L'accès et l'utilisation à l'outil DAAZ s'effectue au moyen d'un ID individuel unique généré automatiquement depuis la plateforme. Cette approche est totalement anonyme et garantit la confidentialité tout au long du parcours. Ainsi, seul l'utilisateur a connaissance de ses avancées et de ses progrès en matière de protection des données. Une fois inscrit, l'utilisateur peut accéder gratuitement à la plateforme, qui est disponible en trois langues : français, anglais et allemand.

LES ACTIVITÉS EN 2024

L'interface intuitive guide les utilisateurs à travers différents modules interactifs, chacun conçu pour renforcer la compréhension et la mise en œuvre des principes et obligations du RGPD. Des quiz et des « challenges » pratiques sont intégrés pour évaluer les connaissances acquises et offrir des documents de mise en conformité adaptés aux besoins spécifiques des PME.

DAAZ propose encore 24 ressources documentaires telles que des fiches pratiques ainsi que 4 scénarios réalistes pour aider les entreprises à naviguer dans les défis quotidiens de la protection des données avec le support de la CNPD, notamment.

En somme, DAAZ est un outil pédagogique innovant qui permet aux PME de renforcer leur conformité au RGPD, afin d'améliorer leur transparence et de consolider la confiance des consommateurs. Grâce à son interface conviviale et à son approche, DAAZ représente une avancée significative dans le domaine de la protection des données pour les petites structures.

Lancement officiel de DAAZ (« Data Accountability from A to Zen »).

4

INTERVIEW

JÉRÔME COMMODI
Chef de projet

MONSIEUR COMMODI, VOUS ÊTES CHEF DE PROJET DE LA PLATEFORME DAAZ. POUVEZ-VOUS NOUS EXPLIQUER L'OBJECTIF DE CET OUTIL ?

L'outil DAAZ est une initiative remarquable de la CNPD, prise en collaboration avec la Luxembourg House of Cybersecurity et le National Cybersecurity Competence Center (LHC-NC3).

Cet outil constituait le principal livrable du projet « DAta Protection CompLiance SupporT TOolkit » (« ALTO »), qui a obtenu

LES ACTIVITÉS EN 2024

en octobre 2022 l'accord de cofinancement de la Commission européenne. Cette proposition avait été soumise dans le cadre de l'appel à projets de la Commission, réservé aux autorités nationales de protection des données, et visant à sensibiliser les parties prenantes tout en renforçant leurs connaissances en matière de législation sur la protection des données (ID CERV-2021-DATA).

L'outil a été conçu pour aider les start-ups et les PME à se conformer au RGPD dans leurs activités quotidiennes de manière « fun », intuitive et gratuite. Grâce à des méthodes de story learning et de learning by doing, DAAZ rend la protection des données accessible et compréhensible, même pour ceux qui ne sont pas experts en la matière.

En somme, la plateforme est une ressource précieuse pour les entreprises souhaitant naviguer dans le paysage complexe de la protection des données, tout en adoptant une approche moderne et engageante.

COMMENT A ÉTÉ CONÇU L'OUTIL DAAZ ?

Le processus de conception de DAAZ a été minutieusement pensé pour mettre l'accent sur l'utilisateur final.

Le développement s'est déroulé en deux phases distinctes sur une période de 20 mois. La première phase a consisté à identifier les besoins spécifiques des PME en matière de protection des données. Pour ce faire, la CNPD a recueilli les avis de 215 entrepreneurs via un questionnaire en ligne.

La deuxième phase a impliqué le développement technique et pédagogique de l'outil, avec l'aide précieuse des développeurs du LHC-NC3 et d'un UX designer recruté par la CNPD pour les besoins de ce projet. Lors de cette phase, la CNPD a décidé de mettre en œuvre les concepts de narration et d'immersion, combinés à la gamification, afin de maximiser l'engagement des utilisateurs et de faciliter leur apprentissage. Cette phase a également inclus des tests avec des PME pour optimiser l'outil et garantir son efficacité.

QUELLES SONT LES PARTICULARITÉS DE L'OUTILS DAAZ ?

L'accès et l'utilisation de l'outil DAAZ se font de manière anonyme au moyen d'un ID individuel unique, généré automatiquement depuis la plateforme. Cette approche garantit une confidentialité totale tout au long du parcours.

Autre point fort de l'outil est sa gratuité et le fait qu'il est disponible en trois langues : français, anglais et allemand.

Comme j'ai mentionné avant, on a misé sur l'immersion et la gamification lors du développement de DAAZ. Des quiz et des « challenges » pratiques sont intégrés pour évaluer les connaissances acquises et offrir des documents de mise en conformité adaptés aux besoins spécifiques des PME.

Enfin, DAAZ propose 24 ressources documentaires, telles que des fiches

pratiques, des templates sous forme de « solutions clés en main », ainsi que 4 scénarios réalistes pour aider les entreprises à naviguer dans les défis quotidiens de la protection des données, avec le soutien de la CNPD.

QUELS SONT LES RETOURS DU TERRAIN QUANT À SON UTILISATION ?

Le retour du terrain est vraiment très positif. En un mot, les utilisateurs de DAAZ parlent d'« engouement ». Ce terme, associé à la protection des données personnelles, illustre parfaitement le travail novateur de la CNPD, centré sur l'utilisateur, pour le développement et le design de l'outil DAAZ.

Au niveau national, DAAZ a su trouver son public. Au 31 décembre 2024 soit, 8 mois après son lancement officiel, la plateforme DAAZ comptait déjà 1338 « users » et 101 « finishers », dépassant largement les attentes de la CNPD.

Au niveau européen, DAAZ est actuellement utilisé en France et Allemagne. De plus, des autorités nationales d'autres pays ont manifesté leur intérêt pour répliquer cet outil.

Sur le plan international, DAAZ a été sélectionné parmi les nominés pour les GPA Global and Privacy Awards 2024, pour la catégorie « Accountability ».

LES ACTIVITÉS EN 2024

CERTIFICATION

La mise en place de mécanismes de certification peut favoriser la transparence et le respect du RGPD et permettre aux personnes concernées de mieux évaluer le niveau de protection de leurs données offert par les produits, services, processus ou systèmes des organisations qui traitent leurs données personnelles. Une certification RGPD ne certifie pas une organisation mais les opérations de traitements faisant l'objet de la certification.

Le cadre d'application pratique de la certification RGPD est développé en concertation avec les autres autorités de contrôle au niveau de l'EDPB (European Data Protection Board) pour assurer une cohérence mais également, au niveau national, en collaboration avec les acteurs intéressés du secteur privé.

La CNPD accorde une grande importance à la certification en tant qu'outil de conformité au RGPD. Elle continue de promouvoir activement les avantages de la certification RGPD, soulignant son rôle crucial dans l'amélioration de la transparence, la confiance des consommateurs et la protection des données personnelles.

Schéma de certification

À ce jour, deux schémas de certification ont été finalisés après leur soumission par la CNPD, en tant qu'autorité chef de file, à l'EDPB :

- *GDPR-CARPA* : Ce schéma de certification RGPD national a été développé par la CNPD.

- *Europrivacy* : Ce schéma de certification européen, dont les critères de certification ont été approuvés par l'EDPB, a été élaboré par le European Center for Certification and Privacy (ECCP), basé au Luxembourg.

La CNPD a reçu une soumission de critères de certification pour un troisième schéma de certification européen en 2024 et a commencé sa revue qu'elle continuera en 2025.

Schéma de certification comme outil de transfert

Fin 2022, la CNPD a reçu une soumission d'un schéma de certification destiné à être utilisé comme outil de transfert (article 46(2)(f) du RGPD). Fin 2023, la CNPD a soumis ce schéma à l'EDPB en tant qu'autorité chef de file pour la phase informelle pour évaluation. Les travaux se sont poursuivis en 2024, avec des efforts continus pour affiner et finaliser ce schéma. Il est important de souligner qu'il s'agit du premier schéma de certification en tant qu'outil de transfert soumis à l'EDPB, marquant une étape significative dans l'établissement d'outils de transfert de données conformes aux exigences du RGPD. Cette initiative pionnière reflète l'engagement de la CNPD à garantir la protection des données personnelles dans les transferts internationaux.

Critères d'agrément pour les organismes de certification

Début 2024, la CNPD a adopté une deuxième série de critères d'agrément destinés aux organismes de certification souhaitant fournir des services de certification dans le cadre de schémas de certification autres que ceux nécessitant la norme ISAE3000 comme méthodologie d'audit (comme c'est notamment le cas du schéma national « GDPR-CARPA »). Ces critères ont fait l'objet d'un avis publié en décembre 2023.

Procédure d'agrément d'organismes de certification

L'agrément a pour objectif d'attester avec l'autorité nécessaire les compétences des organismes de certification, renforçant ainsi la confiance dans le mécanisme de certification. Seul un organisme de certification agréé est habilité à délivrer des certificats dans le cadre d'un schéma de certification RGPD. Une liste avec tous les organismes de certification agréés par la CNPD se trouve sur le site web de la CNPD.

À la fin de l'année 2024, trois organismes de certification ont été agréées pour délivrer

LES ACTIVITÉS EN 2024

le schéma de certification « GDPR-CARPA » développé par la CNPD.

Suite à l'adoption de la deuxième série de critères d'agrément mentionnée plus haut, la CNPD a reçu en 2024 la candidature d'un organisme de certification pour le schéma de certification « Europrivacy » développé par le « European Center for Certification and Privacy » (ECCP, basé au Luxembourg). La CNPD poursuit l'examen de cette candidature en 2025.

Travaux au niveau européen

La CNPD joue un rôle très actif au sein du sous-groupe CEH (Compliance, E-governance & Health) de l'EDPB. En novembre 2024, elle a pris en charge la coordination de ce sous-groupe. Cette responsabilité témoigne de l'engagement continu de la CNPD à promouvoir des pratiques exemplaires en matière de protection des données dans les domaines de la conformité. En coordonnant ce sous-groupe, la CNPD contribue à l'élaboration de lignes directrices et de recommandations qui visent à harmoniser les pratiques de protection des données à travers l'Europe, tout en répondant aux défis spécifiques des acteurs concernés.

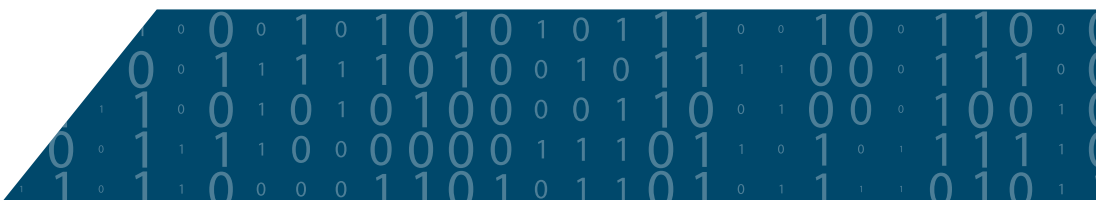
Dans le cadre des travaux de ce sous-groupe, la CNPD s'implique activement dans l'analyse des schémas de certification nationaux et des « European Seals », qui sont soumis à l'EDPB. Cette participation inclut la contribution à la rédaction des opinions de l'EDPB, qui fournissent des orientations et des recommandations sur la conformité des critères de certification avec le RGPD.

En outre, la CNPD est responsable de la coordination d'une équipe dédiée à la création d'une méthode pour examiner les schémas de certification. Cette méthode vise à améliorer l'efficacité et la rigueur des processus d'évaluation au niveau des autorités de protection des données et de l'EDPB, en s'assurant que les schémas de certification soient robustes, transparents et conformes aux exigences du RGPD.

Par ailleurs, la CNPD coordonne un autre groupe de travail dont l'objectif est d'établir une collaboration avec l'association European Accreditation (EA), qui rassemble les organismes nationaux d'accréditation des États membres. Cette collaboration vise à harmoniser au niveau européen les processus de revue des schémas de certification RGPD.

Autres activités au niveau international

En juin 2024, la CNPD a participé avec une grande délégation au Privacy Symposium à Venise, où elle a partagé notamment les leçons tirées de la certification RGPD en Europe, soulignant les défis et les avantages pour les organisations certifiées. Elle y a également abordé le développement de la certification comme outil de transfert de données, particulièrement attendu par les entités hors EEE, et de l'importance de la coopération internationale pour harmoniser les standards de certification en matière de protection des données.



4

CODES DE CONDUITE

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.

Les codes de conduite sont des outils de responsabilisation volontaires qui établissent des règles spécifiques en matière de protection des données pour certaines catégories de responsables de traitement et de sous-traitants. Ils peuvent servir d'instruments de gouvernance utiles et efficaces en fournissant une description détaillée des comportements les plus appropriés et en intégrant les meilleures pratiques d'un secteur donné.

Après une revue approfondie, la CNPD a adopté le 7 novembre 2024 un code de conduite spécifique au secteur du travail intérimaire au Luxembourg. Ce code a été rédigé par le Fonds de formation Sectoriel pour l'Intérim (FSI) qui représente l'ensemble du secteur de l'intérim au Luxembourg. Cette initiative répond à la volonté du secteur de clarifier et de concrétiser la mise en œuvre du RGPD en tenant compte des particularités propres au travail intérimaire.

Procédure d'agrément d'organismes de suivi de codes de conduite

Le 7 novembre 2024, après un audit d'agrément, la CNPD a accordé un agrément à ESCEM asbl en tant qu'organisme de suivi pour le code de conduite du secteur du travail intérimaire au Luxembourg.

Travaux au niveau européen

La CNPD est chargée de la coordination au niveau du sous-groupe CEH des travaux de revue d'un code de conduite international spécifique au domaine du sport. Ces travaux s'inscrivent dans le cadre de la rédaction des recommandations de l'EDPB, visant à assurer que le code de conduite respecte les exigences du RGPD.

LES ACTIVITÉS EN 2024

INTERVIEW

ELENA-CRISTINA GERTH
Chef du service Certifications
et Codes de conduite

MADAME GERTH, VOUS ÊTES CHEF DU SERVICE CERTIFICATIONS ET CODES DE CONDUITE. POUVEZ-VOUS NOUS DONNER UNE IDÉE DES TÂCHES LIÉES À VOTRE POSTE ?

Bien sûr. Je suis en charge de la coordination des activités liées à la mise en œuvre de certifications RGPD, tant au niveau national qu'européen. Ces certifications offrent aux organisations un cadre structuré pour démontrer qu'elles appliquent les principes du Règlement général sur la protection des données dans leurs pratiques quotidiennes.

Je participe régulièrement à des conférences spécialisées, où j'ai l'occasion d'échanger

avec d'autres experts du domaine et de présenter nos travaux, notamment autour du schéma de certification GDPR-CARPA et du label européen Europrivacy, développé au Luxembourg.

Depuis novembre 2024, je coordonne également le sous-groupe « Conformité, e-gouvernement et santé » au sein du Comité européen de la protection des données (EDPB). Ce groupe est également chargé des travaux relatifs à la certification au niveau européen, ce qui nous permet de contribuer activement à l'harmonisation des pratiques à l'échelle de l'UE.

VOUS AVEZ MENTIONNÉ LE SCHÉMA GDPR-CARPA. POUVEZ-VOUS NOUS EN DIRE PLUS ?

GDPR-CARPA est une initiative pionnière de la CNPD, visant à offrir un cadre de certification officiel pour les traitements de données personnelles. Le schéma permet aux responsables de traitement et sous-traitants établis au Luxembourg de démontrer qu'ils appliquent des mesures techniques et organisationnelles conformes au RGPD pour un ou plusieurs traitements spécifiques. Il est également utilisé comme outil de transfert de données personnelles vers des pays tiers.

Nous tirons une grande fierté du succès de GDPR-CARPA, le premier schéma de certification sous le RGPD.

VOTRE SERVICE COMPREND ÉGALEMENT LES CODES DE CONDUITE. QUEL RÔLE CES CODES JOUENT-ILS ?

Les codes de conduite sont des instruments prévus par le RGPD pour aider les responsables de traitement et les sous-traitants à démontrer leur conformité. Ils permettent d'adapter les exigences du RGPD aux spécificités d'un secteur ou d'une activité, tout en assurant un haut niveau de protection des données personnelles.

En effet, la CNPD a récemment approuvé un code de conduite pour le secteur du travail intérimaire qui a été élaboré par le Fonds de Formation Sectoriel pour l'Intérim (FSI) en collaboration avec Fedil Employment Services (FES). C'est une première au Luxembourg !

Au niveau européen, les codes de conduite sont élaborés et adoptés au sein du même sous-groupe chargé des travaux sur la certification.

QUELS SONT LES CRITÈRES POUR QU'UN CODE DE CONDUITE SOIT APPROUVÉ PAR LA CNPD ?

Le code doit démontrer qu'il respecte les principes du RGPD, qu'il est clair, accessible, et qu'il prévoit un mécanisme de suivi efficace. Ce dernier point est crucial : un organisme de contrôle indépendant doit être désigné et agréé par la CNPD afin de s'assurer que les adhérents respectent effectivement les dispositions du code. Par conséquent, l'adhésion à un code reconnu permet de renforcer la confiance des clients et des partenaires, de structurer les pratiques internes, et de bénéficier d'un accompagnement sectoriel. C'est aussi un

LES ACTIVITÉS EN 2024

signal fort envoyé aux autorités de contrôle : l'entreprise s'engage activement dans une démarche de conformité.

VOUS ÊTES ÉGALEMENT MEMBRE DU SOUS-GROUPE « CONFORMITÉ, E-GOUVERNEMENT ET SANTÉ » DE L'EDPB. QUEL RÔLE CE SOUS-GROUPE JOUE-T-IL ?

Comme le dit son nom, le sous-groupe CEH traite des questions de conformité au RGPD dans les domaines de l'e-gouvernement et de la santé. Le groupe de travail joue un rôle stratégique car dans ces secteurs, les enjeux de protection des données sont particulièrement élevés.

Par rapport à l'e-gouvernement, notre objectif est de garantir que les administrations publiques respectent les principes du RGPD lorsqu'elles traitent les données personnelles des citoyens. Ce volet concerne donc la protection des données dans les services publics numériques, tels que les portails administratifs en ligne, les systèmes d'identité numérique, les plateformes de déclaration fiscale ou de sécurité sociale, et les services de vote électronique.

Le deuxième volet se concentre sur la protection des données de santé, qui sont considérées comme des données sensibles. Les discussions du sous-groupe portent notamment sur les systèmes de dossiers médicaux électroniques, les recherches médicales impliquant des données personnelles, les traitements de données dans les hôpitaux et laboratoires, etc.

La majorité de notre travail consiste en l'élaboration de lignes directrices et recommandations pour les autorités nationales de protection des données. Nous analysons également les pratiques des États membres pour assurer une application cohérente du RGPD et collaborons avec d'autres institutions européennes pour harmoniser les approches. Finalement, nous évaluons les projets de certification ou de codes de conduite dans les domaines en question.

En parallèle, le sous-groupe que je coordonne joue un rôle central dans l'analyse de l'articulation entre certains textes du paquet législatif numérique de l'UE et le RGPD (comme Data Governance Act, Data Act, l'EHDS), afin d'assurer une cohérence réglementaire. Ce sous-groupe représente également l'EDPB au sein de l'EDIB (European Digital Identity Board), où j'ai aussi l'honneur d'agir en tant que représentante officielle de l'EDPB.

4

DATA GOVERNANCE ACT (DGA)

En 2024, la CNPD a entamé un projet visant à préparer l'autorité à ses nouvelles responsabilités dans le cadre du Data Governance Act (DGA). En attendant l'entrée en vigueur de la loi luxembourgeoise officialisant ces compétences, la CNPD a mis en place une organisation interne pour se préparer efficacement à ces nouvelles tâches. Ce projet, lancé en 2024, permet de développer les compétences nécessaires et d'anticiper les défis à venir, assurant ainsi une transition fluide et efficace vers ses nouvelles responsabilités.

L'avant-projet de loi 8395A (ci-après dénommé « APL portant création du Commissariat du Gouvernement à la souveraineté des données et désignation des organismes et autorités compétents prévus aux articles 7, 13 et 23 du règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) et du point d'information unique prévu à l'article 8 du règlement (UE) 2022/868 précité, désigne en effet la CNPD comme autorité compétente en matière d'intermédiation de données et d'altruisme des données. La CNPD sera donc l'autorité luxembourgeoise prévisiblement compétente en matière d'intermédiation et d'altruisme des données. Par ailleurs, le DGA introduit un **Comité européen de l'innovation dans le domaine des données** (EDIB, European Data Innovation Board) pour faciliter le partage des bonnes pratiques, en particulier en ce qui concerne l'intermédiation des données, l'altruisme en matière de données et l'utilisation de données publiques qui ne peuvent être mises à disposition en tant que données ouvertes, ainsi que la hiérarchisation des normes d'interopérabilité intersectorielles.

Services d'intermédiation de données : Le partage de données peut impliquer pour une entreprise une perte d'avantage concurrentiel et représente un risque d'utilisation abusive. Le DGA définit un ensemble de règles et un système de notification et de labellisation pour les fournisseurs de services d'intermédiation de données (appelés intermédiaires de données, tels que les places de marché de données) afin de garantir qu'ils fonctionneront en tant qu'organisateurs fiables de partage ou de mise en commun de données au sein des espaces européens communs de données.

Altruisme des données : Les personnes et les entreprises qui donnent leur consentement ou leur permission de mettre à disposition les données qu'elles génèrent – volontairement et sans récompense – pour les utiliser à des fins d'intérêt général pourront autoriser le partage de leurs données par les « organisations altruistes en matière de données reconnues dans l'Union ». Les organisations altruistes doivent avoir un caractère non lucratif et répondre à des exigences de transparence, tout en offrant des garanties spécifiques pour protéger les droits et les intérêts des citoyens et des entreprises qui partagent leurs données.

LES ACTIVITÉS EN 2024

TRANSFERTS INTERNATIONAUX DE DONNÉES PERSONNELLES

Des règles spécifiques s'appliquent aux transferts de données depuis le Luxembourg vers un pays situé en dehors de l'Union européenne ou de l'Espace économique européen (UE, Norvège, Suisse et Liechtenstein). Ces transferts sont autorisés (en dehors de cas limités de dérogations) soit s'il existe une décision d'adéquation concernant le pays tiers en question, soit en utilisant un des outils juridiques prévus par le RGPD pour les transferts internationaux. Certains de ces outils, tels que les mécanismes de certification comme outils de transfert et les règles d'entreprise contraignantes (ou « binding corporate rules »), doivent être revus et approuvés par la CNPD.

Les mécanismes de certification comme outil de transfert

Comme mentionné dans la partie « certification », la CNPD est autorité chef de file pour le premier schéma en tant qu'outil de transfert vers les pays tiers qui a été soumis à l'EDPB en phase informelle en 2024. Dans ce contexte, la CNPD a collaboré étroitement avec les experts du sous-groupe « International Transfers » de l'EDPB pour évaluer les aspects propres aux transferts internationaux des critères de certification proposés. Ces travaux se poursuivront en 2025.

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.

En 2024, la CNPD a travaillé en qualité d'autorité de contrôle chef de file (« lead supervisory authority ») sur six dossiers de demande d'approbation des règles d'entreprise contraignantes (« binding corporate rules ») pour des entreprises multinationales dont l'établissement principal dans l'Espace économique européen est situé au Luxembourg. Un de ces dossiers a été soumis à l'EDPB dans la phase informelle de coopération, où les autorités de l'ensemble des pays membres de l'UE ont eu l'occasion de commenter le dossier pour permettre une interprétation et application harmonisées des exigences du RGPD. Ces dossiers, ainsi que les déclarations annuelles sur la mise à jour des BCR déjà approuvés, continueront à être traités en 2025.

Participation aux travaux de l'EDPB

En 2024, la CNPD a activement participé aux réunions du sous-groupe « International Transfers », au sein de l'EDPB. La CNPD a notamment contribué à la finalisation des FAQ *« EU-US Data Privacy Framework for European individuals »* ainsi que des FAQ *« EU-US Data Privacy Framework for European businesses »* et elle a pris part aux

discussions concernant les lignes directrices 02/2024 sur l'article 48 du RGPD. En outre, la CNPD a été impliquée comme membre du sous-groupe « International transfers » dans le travail sur certains aspects de l'avis de l'EDPB 22/2024 sur les obligations dans le cas d'engagement des sous-traitants et des sous-sous-traitants.

La CNPD a également activement participé en avril 2024 au « BCR workshop » à Vilnius en Lituanie. Ce workshop est organisé tous les deux ans dans le cadre du sous-groupe « International transfers » et a pour objectif de permettre un échange constructif entre les autorités de contrôle dans l'Espace économique européen sur leurs pratiques et d'harmoniser leur approche lors de l'instruction des dossiers BCR.

Lignes directrices sur les transferts internationaux et cadre de protection des données UE-États-Unis

Finalement, la CNPD a procédé à une mise à jour des lignes directrices sur les transferts internationaux. Cette mise à jour a été rendue nécessaire suite aux évolutions récentes des outils de transferts, et notamment à la suite de l'entrée en vigueur du cadre de protection des données UE-États-Unis (« EU-US Data Privacy Framework »).

Dans ce contexte, la CNPD a travaillé sur la mise en place de la possibilité d'introduire des plaintes contre des entreprises américaines certifiées sous le cadre de protection des données UE-États-Unis pour violation de celui-ci ainsi qu'en cas de présomption d'accès illégal par les agences de renseignement américaines à des données personnelles transférées vers les États-Unis. La publication de la nouvelle version des lignes directrices sur les transferts internationaux ainsi que des informations sur la procédure des plaintes sur le site internet de la CNPD est prévue en 2025.

LES ACTIVITÉS EN 2024

7 TRAITER LES RÉCLAMATIONS DES CITOYENS

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.

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

4

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.

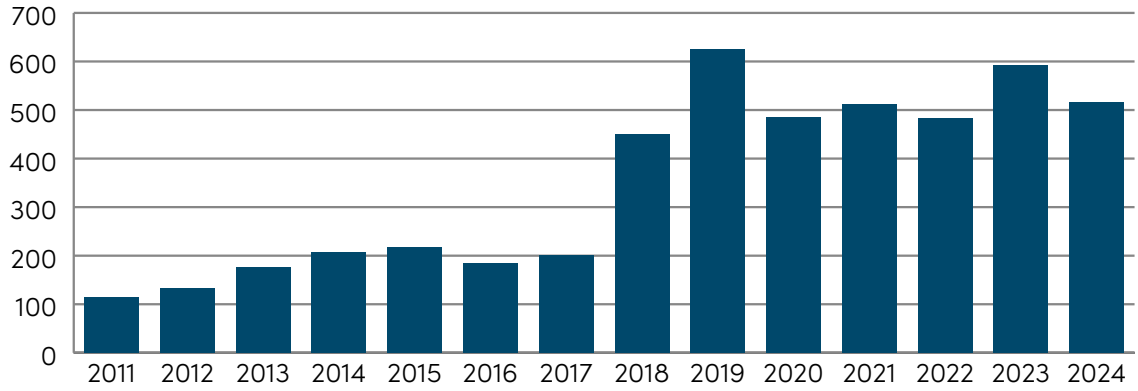
De plus, en fonction des caractéristiques propres à chaque réclamation, la CNPD peut décider d'instruire ou de ne pas instruire une réclamation en tenant compte notamment du degré de gravité des faits allégués, de la violation alléguée, du degré d'impact sur les droits et libertés fondamentaux, du degré de priorité par rapport au nombre de réclamations et des ressources disponibles.

En 2024, la CNPD a reçu un total de 516 réclamations :

- 426 réclamations ont été introduites directement auprès de la CNPD ;
- 90 réclamations ont été traitées via le système européen de coopération (IMI) émanant des autres autorités de contrôle européennes lorsque les responsables du traitement ont leur établissement principal européen au Luxembourg (autorité chef de file).

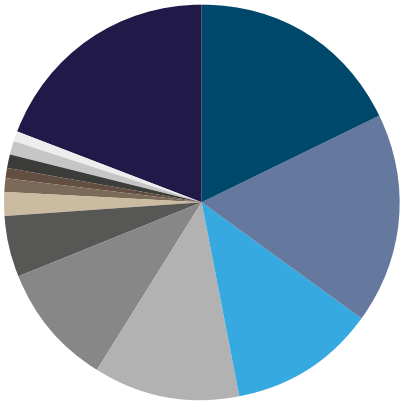
La CNPD a reçu 76 plaintes de moins que l'année précédente. Depuis l'entrée en application du RGPD en 2018, la CNPD traite 524 réclamations en moyenne par année.

ÉVOLUTION DU NOMBRE DES RÉCLAMATIONS



LES ACTIVITÉS EN 2024

MOTIFS DES RÉCLAMATIONS NATIONALES



- Demande d'effacement ou de rectification non respectée (18 %)
- Refus d'accéder aux données (17 %)
- Confidentialité des données / Violation des données (12 %)
- Conformité du traitement (12 %)
- Vidéosurveillance (10 %)
- Opposition à prospection ou plaintes contre le spam (5 %)
- Consultation RNPP (2 %)
- Cookies (1 %)
- Droit à l'image (1 %)
- Droit à l'information (1 %)
- Droit au déréférencement (1 %)
- Géolocalisation(1 %)
- Autres (19 %)

RÉCLAMATIONS NATIONALES

La majorité des réclamations (82 %) était relative à des dossiers nationaux. Il y a eu une diminution de 12 % par rapport à 2023 avec 516 réclamations émanant de citoyens résidents.

Les **demandes d'effacement ou de rectification de données** représentent **18 %** des réclamations adressées à la CNPD. Elles concernent notamment des sollicitations de fermeture de comptes auprès de services ou commerces en ligne, ainsi que des demandes de suppression de données à caractère personnel (adresses e-mail, évaluations, etc.) accessibles sur Internet.

17 % des réclamations portent sur le **non-respect du droit d'accès** par les responsables de traitement. Dans certains cas, ces derniers ont refusé de communiquer tout ou partie des données personnelles, ignoré les demandes ou fourni des informations insuffisantes lors de l'exercice de ce droit.

12 % des réclamations sont liées à des **atteintes à la confidentialité des données** ou à des **violations de données**. Cela inclut, par exemple :

- la publication en ligne de contenus (vidéos, photos, etc.) sans protection adéquate ;
- l'envoi de courriels à des destinataires non concernés, ou l'utilisation du champ « CC » au lieu de « BCC », exposant ainsi les adresses des destinataires.

4

Dans **12 %** des cas, les réclamants ont sollicité la CNPD pour vérifier la **conformité de certaines pratiques administratives ou commerciales**, notamment :

- la collecte excessive ou injustifiée de données ;
- la demande de documents d'identité (carte d'identité, passeport) à des fins de vérification ;
- la publication de données personnelles sur des plateformes en ligne (réseaux sociaux, etc.) ;
- les clauses relatives à la protection des données dans les conditions générales de services ou de commerces en ligne ;
- la durée de conservation des données collectées.

7 % des réclamations concernent des problématiques liées à la **vidéosurveillance**.

5 % sont relatives à l'exercice du **droit d'opposition**, en particulier dans le cadre de la prospection commerciale. La CNPD est intervenue lorsque les liens de désabonnement dans les courriels étaient inopérants ou que les responsables de traitement ne donnaient pas suite aux demandes d'opposition.

Enfin, **2 %** des réclamations visent à vérifier la licéité des consultations effectuées par des agents du secteur public dans le **Registre national des personnes physiques (RNPP)**.

RÉCLAMATIONS EUROPÉENNES DANS LE CADRE DU SYSTÈME DE COOPÉRATION ET DE COHÉRENCE EUROPÉEN

La coopération européenne en matière de réclamations sous le RGPD est supposée garantir une application cohérente des règles de protection des données à travers l'UE. Elle se définit notamment par :

1. **Une coopération entre autorités de contrôle** : Les autorités de contrôle des différents États membres coopèrent étroitement pour traiter les réclamations. L'autorité de contrôle chef de file collabore avec les autres autorités concernées pour parvenir à un consensus et échanger des informations utiles.

2. **Une assistance mutuelle et opérations conjointes** : Les autorités de contrôle peuvent demander une assistance mutuelle et mener des opérations conjointes, notamment pour enquêter ou contrôler l'application des mesures.

3. **Un mécanisme de guichet unique** : Ce mécanisme permet de gérer les plaintes de manière plus efficace en centralisant le traitement des réclamations par une seule autorité de contrôle, même si les données sont traitées dans plusieurs États membres.

4. **Un règlement des litiges** : En cas de désaccord entre les autorités de contrôle, le Comité Européen de la Protection des Données (CEPD) peut intervenir pour

LES ACTIVITÉS EN 2024

régler les litiges et assurer une application cohérente du RGPD.

La CNPD a ainsi traité **90 dossiers** en tant qu'autorité chef de file au cours de la période de référence de 2024. Ces dossiers se répartissent comme suit :

- **31 dossiers** relatifs à la licéité du traitement ou à la sécurité des données.
- **28 dossiers** concernant le droit d'effacement et la rétention des données.
- **25 dossiers** portant sur le droit d'accès.
- **6 dossiers** sur divers autres sujets.

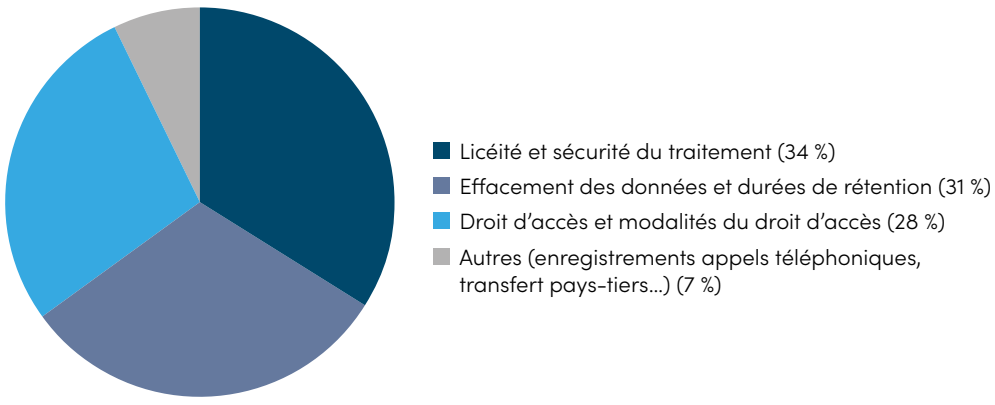
Cette répartition illustre l'engagement continu de la CNPD à garantir la conformité avec le RGPD et à protéger les droits des individus en matière de données personnelles.

DEMANDES DE MISE EN CONFORMITÉ

En 2024, 114 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.

Pour les réclamations au niveau européen, la CNPD a contacté le responsable du traitement pour une prise de position ou une mise en conformité dans 41 dossiers.

MOTIFS DES RÉCLAMATIONS EUROPÉENNES



4

8 ANALYSER LES VIOLATIONS DE DONNÉES

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

- les violations de données dans le cadre du RGPD ; et
- les violations de données dans le secteur des communications électroniques (cf. partie II.3).

VIOLATIONS DE DONNÉES DANS LE CADRE DU RGPD

Le RGPD exige qu'une violation de sécurité entraînant, de manière accidentelle ou illicite, **la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données**, doit être gérée dans le respect des exigences des articles 32, 33 et 34 du RGPD.

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

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer **un risque élevé** pour les droits et libertés d'une personne physique, le responsable du traitement **communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.**

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 donc pas le nombre total d'incidents de sécurité en rapport avec des données à caractère personnel qui se produisent dans les organisations. Toutefois, les responsables du traitement sont tenus de maintenir une documentation de tous les incidents de sécurité impliquant des données à caractère personnel.

En 2024, 442 violations de données ont été notifiées à la CNPD. Cela correspond à une moyenne de presque 37 notifications de violations de données par mois.

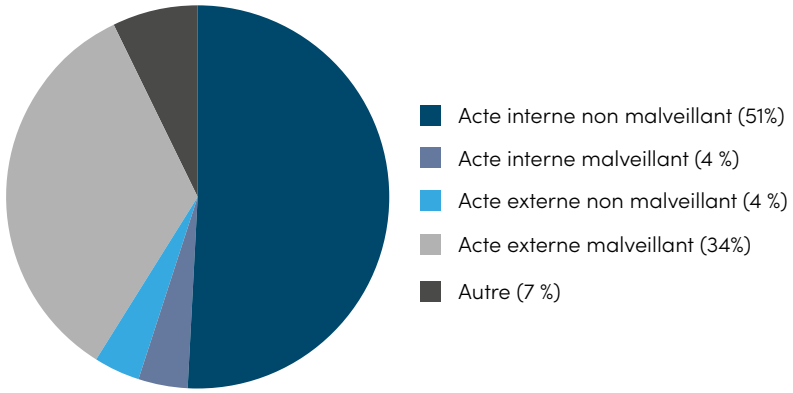
Au total, depuis l'entrée en application du RGPD le 25 mai 2018, la CNPD a reçu 2468 violations de données.

Comme pour les années précédentes, la CNPD a constaté :

- qu'elle ne reçoit que 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.

LES ACTIVITÉS EN 2024

CAUSES DES VIOLATIONS



51 % des cas des violation de données à caractère personnel sont causés par des **erreurs humaines** (acte interne non malveillant).

La plupart des erreurs humaines se produisent :

- lorsqu'une procédure existante n'est pas suivie ;
- lorsqu'une règle de sécurité existante est contournée : ce type de cas a fait l'objet d'incidents aux 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 (p. ex. principe des 4 yeux) aurait probablement permis d'éviter ce type d'incident.

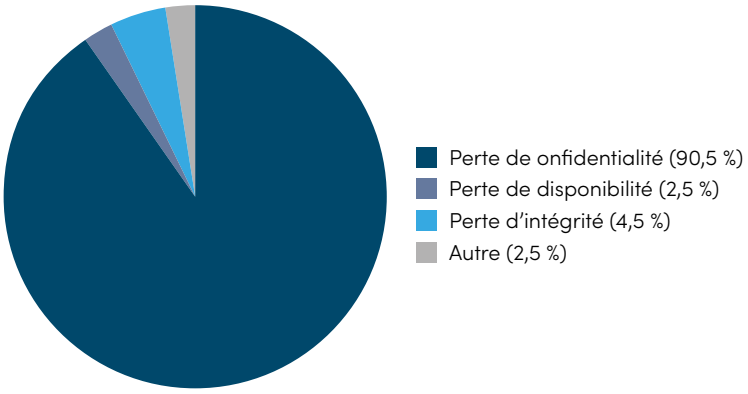
Des **actes externes malveillants** sont à l'origine de plus d'un quart des violations notifiées. Ce type d'incidents a souvent un impact plus important sur les personnes concernées. Dans de nombreux cas, ces actes ciblent l'accès ou l'obtention de données qui permettent de réaliser des transactions financières à l'insu des personnes concernées (p. ex. interception de données de cartes de paiement bancaire, phishing pour obtenir les informations de connexion 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.

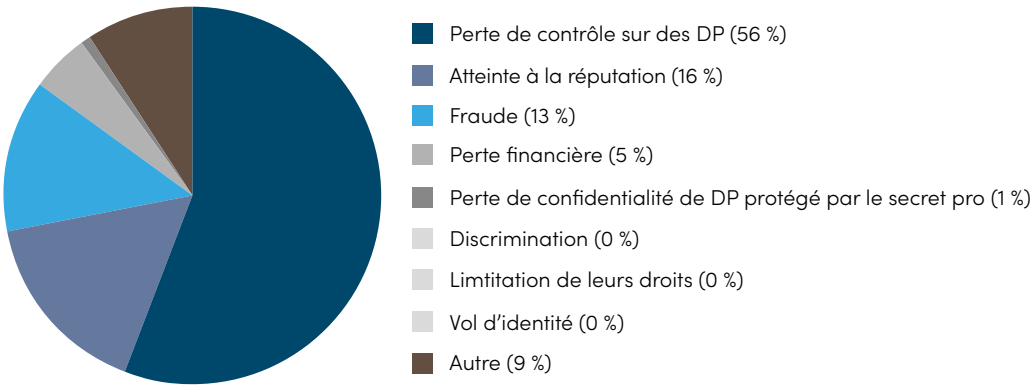
Les autres cas de figure sont liés à des bugs techniques qui résultent souvent dans la divulgation de données à caractère personnel à des tiers non autorisés (p. ex. mise en place ou mise à jour d'un nouveau service en ligne, cas non prévu d'utilisation d'un service, etc.).

NATURE DE L'IMPACT



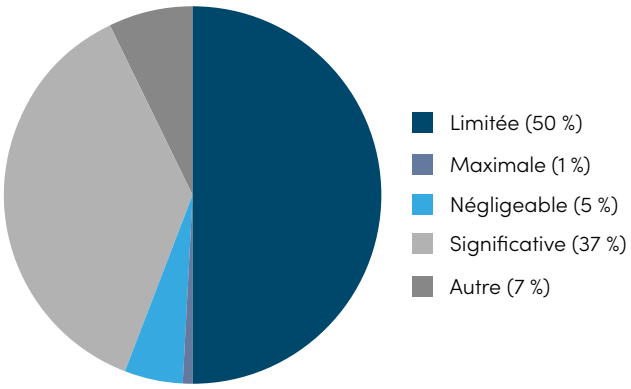
La quasi-totalité des violations de données ont un impact en rapport avec la perte de confidentialité des données concernées. Il est à noter l'apparition de cas mixtes concernant les attaques de type « ransomware » qui combinent une perte de disponibilité mais aussi de plus en plus régulièrement une perte de confidentialité suite à l'exfiltration partielle ou totale des données afin de les publier sur le dark web. 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.

LES ACTIVITÉS EN 2024



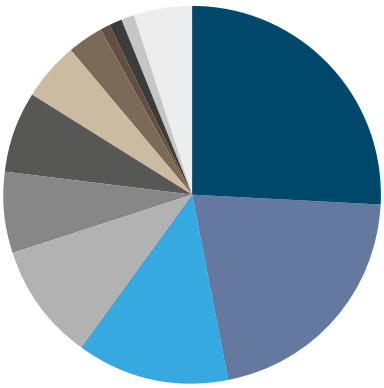
La CNPD attire également l'attention des responsables du traitement sur le fait qu'un certain nombre d'actes de piratage et de phishing sont ciblés sur le personnel de la direction d'une organisation et leur entourage (p. ex. assistant/secrétariat de la direction). Ces actes malveillants ont souvent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

SÉVÉRITÉ DE L'IMPACT



4

NATURE DES INCIDENTS



- Piratage, hacking (26 %)
- Divulgation au mauvais destinataire (21 %)
- Divulgation de données personnelles de la mauvaise personne (13 %)
- Dispositif perdu ou volé (10 %)
- Erreur de setup (7 %)
- Problème technique (7 %)
- Publication involontaire (5 %)
- Papiers perdus, volés, endroit non sécurisé (3 %)
- Communication verbale non autorisée (1 %)
- Mail perdu, ouvert (1 %)
- Malware, logiciel malicieux (1 %)
- Autre (5 %)

LES ACTIVITÉS EN 2024

9 RECEVOIR LES SIGNALEMENTS DU TYPE « WHISTLEBLOWING »

En tant qu'une des 22 autorités compétentes désignées par la législation sur les lanceurs d'alertes, la CNPD met à disposition sur son site internet un canal de signalement externe, permettant de signaler en toute confidentialité des préoccupations sérieuses concernant des violations potentielles en lien avec la législation sur la protection des données à caractère personnel.

Cet outil est conçu pour permettre à toute personne, qu'elle soit employée ou non de l'organisation en question, de signaler des problèmes graves liés à la protection des données personnelles au sein de cette organisation. Cela pourrait inclure des incidents tels que des violations de la confidentialité des données, des failles de sécurité informatique ou tout autre aspect préoccupant concernant la manipulation ou l'utilisation non autorisée de données personnelles.

La CNPD tient à souligner les points suivants concernant l'utilisation de ce canal de communication des signalements :

- **Confidentialité** : Toutes les informations fournies lors d'un signalement seront traitées de manière strictement confidentielle. Les détails ne seront divulgués qu'aux personnes impliquées dans l'enquête sur le principe du « need to know ». Le système mis à disposition offre un haut niveau de confidentialité. Le choix est donné à l'auteur d'un signalement de le transmettre de manière totalement anonyme ou en s'identifiant.

- **Responsabilité** : Les organisations doivent répondre de manière responsable aux signalements concernant des problèmes de sécurité des données. La CNPD, avec les autres autorités compétentes identifiées dans la législation sur les lanceurs d'alerte, travaillera en collaboration avec les entreprises pour enquêter sur les incidents signalés et garantir des mesures correctives appropriées.

La CNPD a mis en ligne une FAQ[6] (« Foire aux questions ») pour les lanceurs d'alerte sur son site internet.

[6] https://cnpd.public.lu/fr/support/lanceurs-alerte.html

4

10 CONTRÔLER ET ADOPTER DES MESURES CORRECTRICES

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 1er août 2018 précitée. Il soumet cette proposition au Collège qui l'approuve endéans un délai d'un mois à la majorité des voix et qui désigne un membre du Collège, à l'exception du président, en tant que chef d'enquête.

Le dossier d'enquête est alors instruit par le chef d'enquête sur base des informations, déclarations et/ou pièces collectées lors de l'enquête y compris au moyen des éventuels entretiens et/ou demandes d'informations complémentaires. À 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 ensuite 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 1er août 2018, c'est-à-dire d'ordonner la publication d'une décision de manière intégrale et nominative.

LES ACTIVITÉS EN 2024

La Commission nationale dispose de certains 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 règlementation, la CNPD peut adopter des mesures correctrices y inclus des amendes financières.

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 différentes formes, notamment : de manière annoncée ou non, sur dossier, sous forme de visite sur place ou encore sous forme d'audit.

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 (hors domiciles privés), notamment toute installation et tout moyen de traitement.

Tel qu'annoncé dans le rapport annuel précédent, la division enquête a été partiellement restructurée. Elle est à présent composée de deux services dont l'un a pour mission de réaliser les enquêtes à proprement parler, tandis que l'autre analyse les opérations en amont, notamment grâce au mécanisme interne « d'alerte », et en aval, notamment par le biais de communications publiques.

À la fin de l'année 2024, la division gérait 44 dossiers actifs dont 29 avaient été ouverts en 2024.

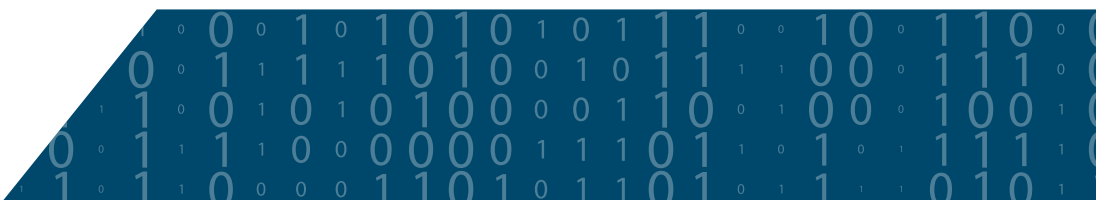
Les deux axes de contrôles récurrents validés en 2023, à savoir le contrôle des systèmes de vidéosurveillance dans les lycées et le contrôle des registres des traitements, ont donné lieu à l'ouverture de 10 enquêtes en 2024 et constituent la majorité des dossiers actifs en 2024.

Par ailleurs, plusieurs enquêtes réactives ont été ouvertes sur des thématiques tels que la vidéosurveillance, l'exercice du droit d'accès ou encore la prospection commerciale.

Sur le plan des analyses, les alertes reçues proviennent aussi bien de la division Réclamations, à travers son service réclamations nationales et son service signalements, que de la division Guidance. Les alertes portent sur des sujets variés tels que les failles de sécurité, le recueil du consentement, le détournement de finalité et évidemment la vidéosurveillance.

Deux communications publiques ont été réalisées en lien avec la division enquête, l'une sur les activités de surveillance de la CNPD dans le contexte de la pandémie de Covid 19, l'autre sur les enquêtes thématiques relatives à la transparence dans le secteur du e-commerce.

Finalement, la fin de l'année 2024 a marqué le déploiement d'une opération d'envergure portant sur l'obligation de désignation d'un délégué à la protection des données à



l'attention des organismes publics. Dans le cadre de cette opération, 20 organismes ont déjà été contactés et l'action se poursuivra tout au courant de l'année 2025.

DÉCISIONS SUR L'ISSUE DES 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 du RGPD par le responsable du traitement 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 1er août 2018 portant organisation de la

LES ACTIVITÉS EN 2024

Commission nationale pour la protection des données et du régime général sur la protection des données.

Avant que ladite formation restreinte ne prenne 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.

La Commission nationale siégeant en formation restreinte a adopté 3 décisions sur l'issue d'enquêtes en 2024: 1 décision de clôture en l'absence de manquements retenus et 2 décisions avec mesures correctrices dont 1 avec amende administrative.

Tous les dossiers concernaient des affaires purement nationales avec un total de 2 300 € d'amende administrative.

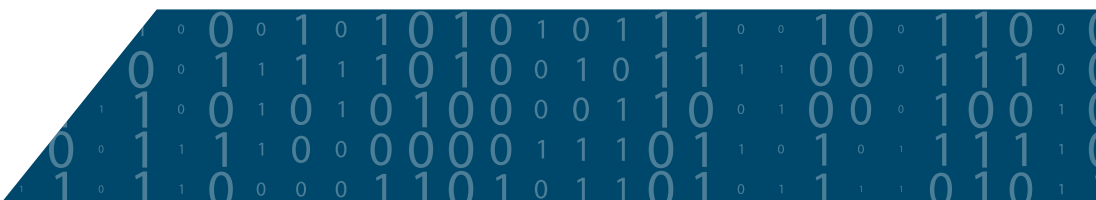
Des 3 dossiers, une décision concernaient une enquête relative au respect de l'article 30 du RGPD relatif au registre des activités de traitement, celle-ci a été clôturée n'ayant pas révélée une violation du RGPD ou de la loi du 1er août 2018 précitée.

Les deux autres dossiers concernaient des traitements de données à caractère personnel opérés à travers des dispositifs de vidéosurveillance. Dans un dossier un rappel à l'ordre a été prononcé par la Commission nationale siégeant en formation restreinte au regard d'un manquement à l'article 5.1.b) du RGPD (principe de la limitation des finalités). Finalement, dans l'autre dossier la Commission nationale siégeant en formation restreinte a retenu que les dispositions de l'article 6.1 (principe de licéité), l'article 5.1.a) lié aux articles 13.1 et 13.2 (principe de transparence et obligations d'information), l'article 5.2 lié à l'article 24.1 (principe et obligation de responsabilité), l'article 5.1.e) (principe de la limitation de la conservation) et l'article 32.1 (sécurité du traitement) du RGPD n'ont pas été respectées. Elle a prononcé deux mesures correctrices (un ordre de limitation du traitement et un ordre de mise conformité) et une amende administrative.

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 3 mois.

Toutefois, en application de l'article 42 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la CNPD est tenue au secret professionnel qui l'empêche de communiquer en détail sur un dossier spécifique.

En outre, sans préjudice de l'article 52 précité de ladite loi, la CNPD publie en principe sur son site Internet ses décisions de façon pseudonymisée et ceci même avant que les voies de recours ne soient épuisées, hormis les décisions pour lesquelles une publication n'est pas envisageable en raison d'un risque élevé de réidentification du contrôlé.



4

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

En application de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, la CNPD est aussi compétente pour contrôler les traitements de données opérés par les autorités répressives ou les autorités de sécurité nationale, telles que la Police grand-ducale, le Service de renseignement de l'État, l'Autorité nationale de sécurité ou l'Administration des douanes et accises.

L'article 10 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit par ailleurs que le rapport annuel de la CNPD doit comprendre une liste des types de violations notifiées et des types de sanctions imposées en vertu de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Au cours de l'année 2024, la CNPD a participé à 8 réunions du sous-groupe Border Travel Law Enforcement de l'EDPB. Une présentation détaillée des activités de la CNPD concernant sa participation à l'EDPB peut être trouvée dans la partie II.5.

LES ACTIVITÉS EN 2024

1 DEMANDES D'INFORMATION

Parmi les demandes d'information traitées en 2024, 3 avaient comme sujet le traitement de données dans le domaine répressif et de sécurité nationale..

2 AVIS

Parmi les avis adoptés par la CNPD, 6 avis étaient relatifs aux traitements de données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Une présentation détaillée des activités de la CNPD concernant les avis peut être trouvée dans la partie *Intervenir dans le processus législatif* sur la page 32.

3 RÉCLAMATIONS

En 2024, la CNPD n'a pas été saisie de réclamation en matière pénale et de sécurité nationale.

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.

Parmi les notifications reçues en 2024, 1 relevait de la matière pénale et de sécurité nationale. Une présentation détaillée des activités de la CNPD concernant les notifications de violation de données peut être trouvée dans la partie *Analyser les violations de données* sur la page 75.

4

LES ACTIVITÉS DANS LE CADRE DE LA SUPERVISION COORDONNÉE DES SYSTÈMES D'INFORMATION À GRANDE ÉCHELLE DE L'UE ET DES ORGANES, OFFICES ET AGENCES EUROPÉENNES

La supervision coordonnée du traitement des données dans les systèmes d'information à grande échelle de l'UE et des organes, offices et agences de l'UE dans les domaines des frontières, de l'asile et des migrations (VIS, Eurodac), de la coopération policière et judiciaire (SIS, Parquet européen, Eurojust, Europol) et du marché intérieur (IMI) est assurée par les groupes de coordination. Dans ce contexte, la CNPD participe aux réunions desdits groupes de coordination et doit effectuer des audits réguliers et des actions coordonnées entre les autorités de protection des données sur les traitements nationaux.

Les tâches des groupes consistent, notamment, à soutenir les autorités de contrôle dans la réalisation d'audits et d'inspections, à examiner les difficultés d'interprétation ou d'application des actes juridiques de l'UE concernés et de propositions de solutions harmonisées, à étudier les problèmes liés à l'exercice d'un contrôle indépendant ou à l'exercice et la promotion des droits des personnes concernées.

LES ACTIVITÉS EN 2024

Au cours de l'année 2024, la CNPD a participé à 9 réunions des groupes de coordination ainsi que 9 réunions de sous-groupes respectivement « drafting team meetings ».

1 SYSTÈME D'INFORMATION SCHENGEN (SIS)

En ce qui concerne le système d'information Schengen (SIS), la CNPD a lancé en août 2024, un nouvel audit récurrent. Cet audit porte dans un premier temps sur la répartition des tâches et rôles dans la nouvelle version du SIS et dans un deuxième temps sur la gestion des accès au SIS.

Parmi toutes les réclamations reçues en 2024, 2 étaient en relation avec le SIS.

Parmi toutes les demandes d'informations reçues en 2024, 13 étaient en relation avec le système d'information Schengen.

2 SYSTÈME D'INFORMATION SUR LES VISAS (VIS)

En ce qui concerne le système d'information sur les visas (VIS), la CNPD a clôturé l'audit de la mission diplomatique et consulaire à Washington DC lancé en 2023. Elle a par ailleurs lancé et clôturé un audit sur les traitements des données effectuées par l'autorité centrale des visas.

Parmi toutes les demandes d'informations reçues en 2023, aucune n'était en relation avec le VIS.

3 EUROPOL

Sur base d'une action commune, la CNPD a continué un contrôle de légalité des transferts de données vers Europol en ce qui concerne le traitement de données de mineurs en dessous de 15 ans qualifiés de suspects.

4 MÉCANISME D'ÉVALUATION ET DE SUIVI DE SCHENGEN (SCHEVAL)

Les autorités de contrôle européennes en matière de protection des données sont amenées à apporter leurs expertises pour le mécanisme d'évaluation et de suivi de Schengen (SCHEVAL) utilisé pour contrôler la mise en œuvre de l'acquis de Schengen - ensemble commun de règles de Schengen qui s'appliquent aux États membres de l'UE. En 2024, la CNPD a participé en tant qu'expert à l'évaluation de la Slovaquie.

5 AVIS

Parmi les avis adoptés par la CNPD, 1 avis était relatif à un projet de loi visant à accompagner l'entrée en application des règlements européens portant refonte au SIS.

4

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) N°611/2013 de la Commission européenne du 24 juin 2013, les fournisseurs de services de communications électroniques accessibles au public, tels que les entreprises de téléphonie fixe/mobile ou les fournisseurs d'accès à l'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 2024, aucune violation de données dans le secteur des communications électroniques n'a été signalée à la CNPD.

LES ACTIVITÉS EN 2024

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 a contribué en 2024 aux travaux de nombreux organismes au niveaux 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 nationales de protection des données, 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 (Global Privacy Assembly ou GPA) ;
- de la Conférence de printemps avec son séminaire « European Case Handling Workshop » ;
- du « Groupe de Berlin », dédié à la protection des données dans le secteur des communications électroniques ;
- de l'Association francophone des autorités de protection des données personnelles (AFAPDP) ;
- du Comité de la Convention 108 (T-PD) du Conseil de l'Europe.

1 COMITÉ EUROPÉEN POUR LA PROTECTION DES DONNÉES (EUROPEAN DATA PROTECTION BOARD OU EDPB)

L'EDPB est un organe européen indépendant, établi par le RGPD, qui a pour mission de veiller à l'application cohérente des règles en matière de protection des données dans l'Union européenne (UE). L'EDPB atteint cet objectif en encourageant la coopération entre les autorités de contrôle nationales et en publiant des orientations générales à l'échelle de l'UE sur l'interprétation et l'application des règles en matière de protection des données.

Le Comité européen est composé des responsables des autorités de contrôle de l'UE et du contrôleur européen de la protection des données (EDPS). Les autorités

de contrôle des pays de l'EEE (l'Islande, le Liechtenstein et la Norvège) sont également membres de l'EDPB, mais n'ont pas de droit de vote. La Commission européenne et, en ce qui concerne les sujets liés au RGPD, l'Autorité de surveillance de l'Association européenne de libre-échange, ont le droit de participer aux activités et aux réunions de l'EDPB.

L'EDPB a son siège à Bruxelles et y dispose d'un secrétariat, qui est assuré par l'EDPS. Un protocole d'accord fixe les modalités de la coopération entre l'EDPB et l'EDPS.

L'EDPB 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.

PROGRAMME DE TRAVAIL 2024-2025

Début octobre 2024, l'EDPB a publié son programme de travail biennal pour 2024 et 2025 sur la base de la stratégie du Comité et des besoins recensés par les membres comme une priorité. L'EDPB entend prendre des mesures importantes pour être en accord avec la stratégie 2024-2027 et les besoins des acteurs, à savoir :

- Renforcer l'harmonisation et faciliter le respect des règles (pilier 1),
- Promouvoir une application effective des règles et une coopération efficace entre les autorités nationales de surveillance (pilier 2),
- La sauvegarde de la protection des données à caractère personnel dans le contexte d'interrégulation et du développement digital (pilier 3) et
- Promouvoir les discussions sur la protection des données à caractère personnel au niveau mondial (pilier 4).

RÉUNIONS PLÉNIÈRES ET REPRÉSENTATION AU SEIN DES SOUS-GROUPES DE TRAVAIL

En 2024, le Comité a organisé 12 réunions plénières. Cinq réunions avaient lieu à Bruxelles, en présentiel, et 7 à distance. La CNPD, représentée à chaque fois par un de ses commissaires, a participé à toutes ces réunions plénières.

La CNPD a également été représentée au sein des 13 sous-groupes thématiques de travail et des cinq « taskforces » constitués pour mener à bien des missions spécifiques du Comité. Ainsi, tout au long de l'année, la CNPD a participé à 126 réunions des sous-groupes de travail et 35 réunions des task-forces, sans compter des nombreuses réunions en équipe de rédaction.

LES ACTIVITÉS EN 2024

Procédures de règlement des litiges du Comité

En 2024, le Comité n'a pas rendu de décisions contraignantes sur base des articles 65 ou 66 (2) du RGPD, mécanisme qui permet de garantir l'application cohérente du RGPD par les autorités nationales de contrôle de la protection des données.

Comité de Supervision Coordonnée (CSC)

La CNPD représente également le Luxembourg dans les réunions biannuelles du CSC.

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

Le CSC doit assurer la supervision coordonnée des systèmes d'information à grande échelle et des organes et organismes de l'UE, conformément à l'article 62 du règlement (UE) 2018/1725 ou à l'acte juridique de l'UE portant création du système d'information à grande échelle ou de l'organe ou organisme de l'UE.

Les tâches du CSC 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.

Les systèmes d'information à grande échelle, organes et agences d'information de l'UE suivants relèvent actuellement du champ d'application du CSC :

- Système d'information du marché intérieur (IMI),
- Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust),
- Parquet européen (EPPO),
- Agence de l'Union européenne pour la coopération des services répressifs (Europol),
- Système d'information Schengen (SIS).

Les autorités nationales chargées de la protection des données, dont la CNPD, supervisent l'application des règles en matière de protection des données dans leurs pays respectifs, tandis que l'EDPS contrôle la manière dont les règles en matière de protection des données sont appliquées au niveau central. Les deux niveaux collaborent pour assurer une surveillance coordonnée de bout en bout.

Les représentants des autorités nationales chargées de la protection des données

peuvent participer aux activités du CSC concernant un système d'information à grande échelle spécifique ou un office, un organe ou une agence de l'UE, uniquement lorsque leur pays respectif applique l'acte juridique de l'UE établissant le système d'information à grande échelle ou l'office, l'organe ou l'agence de l'UE.

Le Luxembourg applique tous les actes juridiques des systèmes d'information à grande échelle ou des offices, organes ou agences de l'UE susmentionnés. La CNPD participe donc à toutes les activités du CSC.

À l'avenir, il est prévu que les systèmes informatiques à grande échelle suivants entrent également dans le champ d'application du CSC :

- Système d'entrée/sortie (EES),
- Système européen d'information et d'autorisation concernant les voyages (ETIAS),
- Système européen d'information sur les casiers judiciaires des ressortissants de pays tiers (ECRIS-TCN),
- Système d'information sur les visas (VIS),
- Base de données dactyloscopiques européennes en matière d'asile (EURODAC),
- Système d'information douanier (CIS),
- Interopérabilité de l'EES, de l'ETIAS, de l'ECRIS-TCN, d'EURODAC, du SIS et du VIS.

2 GLOBAL PRIVACY ASSEMBLY

En octobre 2024, a eu lieu à Jersey la 46ème réunion annuelle des membres de la GPA provenant de plus de 80 pays. Quatre importantes résolutions ont été adoptées lors de cette réunion :

1. *Resolution Endorsing and Encouraging the Use of Data Protection Certification Mechanisms ;*
2. *Resolution on principles regarding the processing of personal information in neuroscience and neurotechnology ;*
3. *Resolution on Data Free Flow with Trust and an effective regulation of global data flows ;*
4. *Resolution on the GPA Rules & Procedures.*

La CNPD a contribué aux travaux des groupes de travail suivants :

- Groupe de travail sur l'économie numérique ;
- Groupe de travail sur l'éducation numérique ;
- Groupe de travail sur le rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide internationale humanitaire et la gestion de crise.

LES ACTIVITÉS EN 2024

LE « DIGITAL EDUCATION WORKING GROUP »

La priorité de ce groupe de travail est de sensibiliser le jeune public, les enfants, les adolescents, les enseignants 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.

Ce travail collaboratif 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, responsable du groupe de travail, et la CNPD, en tant que responsable technique pour l'outil sur CIRCABC, ont continué à réorganiser la plateforme de ressources afin de mettre à jour et d'améliorer la qualité, la présentation et la diffusion du contenu de la bibliothèque tout en respectant une nouvelle classification par types de support d'enseignement et de formation et en y ajoutant des rubriques complémentaires pour répondre aux attentes actuelles.

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 la vie privée des citoyens, bandes dessinées, jeux en ligne. Ces supports sont destinés aux différents publics concernés, à savoir les enseignants et le personnel éducatif, les parents, les enfants et les jeunes par groupes d'âge.

Pour accélérer le renouvellement, 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.

Par ailleurs, un projet d'étude qualitative est en préparation concernant le rôle clé des professionnels de l'éducation en matière de sensibilisation et de formation à la protection des données de leurs élèves. Cette étude interrogera les enseignants de tous les niveaux de classes sur :

- la perception qu'ils ont de leur connaissance et intérêt pour les sujets liés à la protection des données, et de la sensibilisation à des usages numériques responsables de leurs élèves dans leurs cours ;
- leurs attentes pour mieux traiter ces sujets.

4

3 CONFÉRENCE DE PRINTEMPS DES AUTORITÉS EUROPÉENNES À LA PROTECTION DES DONNÉES (SPRING CONFERENCE)

La CNPD a participé à la 32ème édition de la Conférence de Printemps des autorités européennes de protection des données qui a eu lieu en Lettonie, à Riga, du 14 au 16 mai 2024. Les riches discussions entre les représentants des autorités portaient, entre autres, sur le rôle des autorités de la protection des données dans l'ère des nouvelles régulations, la sauvegarde des données de santé dans le cadre de la digitalisation, les défis liés à l'application des règles relatives à la lutte contre le blanchiment et le financement du terrorisme et le RGPD.

Une résolution a été adoptée lors de la Conférence de Printemps, à savoir la « Resolution on enhanced cooperation and establishment of working groups for data protection authorities ».

4 EUROPEAN CASE HANDLING WORKSHOP (ECHW)

L'ECHW 2024 s'est déroulé du 4 au 6 décembre 2024 à Tallin, en Estonie. Cet événement annuel est un forum de dialogue participatif entre les autorités de contrôle de protection des données de l'EEE afin d'aborder ensemble les défis auxquels ces autorités sont confrontées et les solutions qu'elles appliquent dans leur pratique quotidienne.

À cette occasion, les agents de la CNPD ont animé un workshop destiné à discuter des problématiques rencontrées dans la gestion des réclamations, en particulier des aspects techniques et juridiques des sujets liés aux pratiques de vidéosurveillance.

LES ACTIVITÉS EN 2024

5 GROUPE DE BERLIN

Deux réunions du Groupe de travail international sur la protection des données dans les télécommunications (dit « Groupe de Berlin ») ont été organisées en 2024. La première a eu lieu à Oslo, en Norvège, en juin 2024. Les discussions techniques se sont concentrées sur la protection des données à l'ère de l'intelligence artificielle, la reconnaissance faciale et les nouvelles neurotechnologies.

La seconde réunion du Groupe de Berlin s'est tenue à Bruxelles, en Belgique, en novembre 2024. Les discussions fructueuses ont porté notamment sur les méthodes d'apprentissage pour les modèles d'intelligence artificielle ou l'appréhension des modèles d'IA génératives.

Groupe de Berlin.

4

6 ASSOCIATION FRANCOPHONE DES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES (AFAPDP)

La CNPD a participé à la 16ème Assemblée générale ordinaire et extraordinaire de l'AFAPDP, tenue le 28 octobre 2024 à Jersey. Cette réunion a permis d'adopter plusieurs décisions importantes, notamment la révision des statuts de l'association, l'élection d'une nouvelle Présidente (île Maurice), et l'approbation des rapports financier et moral.

Un appel à intérêt a été lancé afin de sélectionner les experts qui accompagneront l'autorité malgache dans la première phase de mise en place de son cadre de protection des données personnelles. Par ailleurs, les membres ont échangé sur les moyens d'appuyer les autorités francophones disposant d'une législation, mais rencontrant des difficultés dans sa mise en œuvre effective.

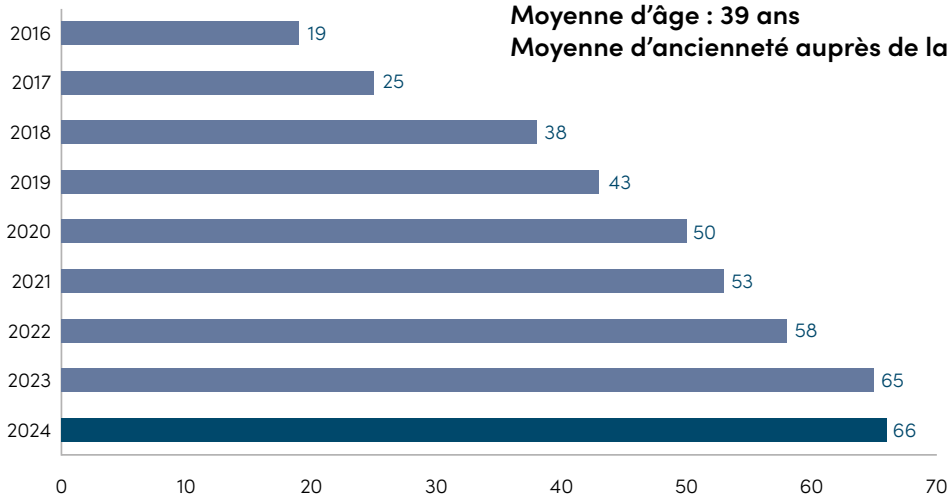
7 COMITÉ DE LA CONVENTION 108 (T-PD) DU CONSEIL DE L'EUROPE

En 2024, la CNPD a participé à la 46ème et à la 47ème réunion plénière du Comité de la Convention 108. Les réunions du Comité veillent à la bonne application et à une interprétation harmonisée des dispositions de la Convention 108 à la lumière des nouveaux défis. En 2024, le Comité a notamment travaillé sur des lignes directrices sur le traitement des données à caractère personnel dans le contexte des neurosciences et a adopté le troisième module des clauses contractuelles types pour le transfert de données personnelles de sous-traitant à sous-traitant.

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

1 RESSOURCES HUMAINES

Moyenne d'âge : 39 ans
Moyenne d'ancienneté auprès de la CNPD : 5 ans



5

COLLÈGE

Tine A. LARSEN,
Présidente

Thierry LALLEMANG,
Commissaire

Marc LEMMER,
Commissaire

Alain HERRMANN,
Commissaire

MEMBRES SUPPLÉANTS

Michèle BRAM,
Juriste

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

Marc HEMMERLING,
Licencié et Maître en Informatique

François THILL,
Conseiller au Ministère de l'Économie, Direction générale Industrie, nouvelles technologies et recherche, Responsable cellule cybersécurité

SECRÉTARIAT GÉNÉRAL DU COLLÈGE

Dani JEITZ,
Secrétaire générale

Claudia FETZ,
Juriste

Kathrin KRAEMER,
Juriste

Marie DOUZAL,
Chef de service « Avis textes légaux »

Nathalie WANGEN,
Juriste

Patrizia ROSA,
Auditeur, Gestionnaire de projets

Bertrand NAVARRE,
Délégué à la protection des données

Christian WELTER,
Assistant au délégué à la protection des données

Solène BENNET,
Chargée des relations européennes et internationales

Tom KAYSER,
Chargé de communication

DIVISION ADMINISTRATION

Thierry RIES,
Chef de division

Patricia SCHOLER,
Chef de service « Accueil et installations »

Estelle DE MUYSER,
Agent administratif

Cristina FERNANDES,
Rédacteur

Maryse WINANDY,
Chef de service « Ressources humaines »

Zoé BECKER,
Rédacteur, Comptabilité & Finances

Jan KUFFER,
Chef de service « Informatique & Logistique »

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

DIVISION GUIDANCE

Arnaud HABRAN,
Chef de division

Jérôme COMMODI,
Chef de projets

Vanessa BEMTGEN,
Juriste, Demandes d'informations

Céline DEROOSE,
Juriste, Demandes d'informations

Aurélie LAGOUTTE,
Juriste, Demandes d'informations

Ovidiu SIMION,
Juriste, Demandes d'informations

Aleksandra GUCWA,
Chef de service « Lignes directrices thématiques »

Alexandre KUHN,
Chef de service « Formation »

Tom KAYSER,
Chef de service « Communication et Connaissances »

Ryan DUCHENE,
Infographiste

Vincent LEGELEUX,
Expert IT

Stéphanie MATHIEU,
Rédacteur

Myriam WECKER,
Expert en communication

DIVISION CONFORMITÉ

Christine ANDRES,
Chef de division

Elena-Cristina GERTH,
Chef de service « Certification & Codes de conduite »

Maxime BAHL,
Juriste

Nina BURMEISTER,
Chef de service « Audits & Analyses d'impact »

Maxime DUFOUR,
Juriste

Kalliroi GRAMMENOU,
Chef de service « Transferts pays tiers »

Regina DECOVILLE,
Juriste

DIVISION RÉCLAMATIONS

Laurent MAGNUS,
Chef de division

Nicolas RASE,
Chef de service « Réclamations nationales »

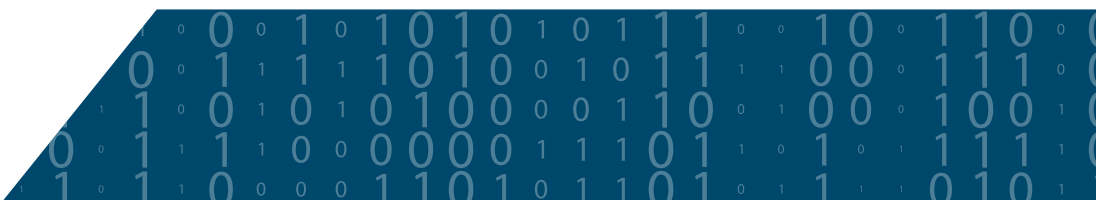
Joël BOUCHER-DE MUYSER,
Juriste

Gaël DUMORTIER,
Juriste

Barbara GIROUD,
Juriste

Isabel SUBIRATS,
Juriste

Georges WEILAND,
Chef de service « Réclamations européennes »



5

Sabrine ABAAB,
Juriste

Victor BOJKO,
Juriste, Réclamations européennes

Cédric HACK ROLLMANN,
Juriste

Jessica WINKLER,
Juriste

Maximilian WELSCH,
Chef de service « Signalements »

Sébastien TEISSEIRE,
Expert IT

DIVISION ENQUÊTES

Michel SINNER,
Chef de division

Florent KLING,
Chef de service « Opération des contrôles »

Edith MALHIERE,
Chef de service « Analyse des contrôles »

Estelle BURET,
Chargée d'instruction

Marc MOSTERT,
Enquêteur

Bao-Khanh NGUYEN TRUNG,
Enquêteur

Marie-Laure FABBRI,
Enquêteur

Margot GILLMANN,
Chargée d'instruction

Diana FERREIRA,
Chargée d'instruction

François RICHALET,
Enquêteur

Amandine THER,
Chargée d'instruction

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

ASSERMENTATION DE FONCTIONNAIRES

En 2024, Madame Tine A. Larsen, Présidente de la CNPD, a procédé à l'assermentation de

- Monsieur François Richalet, nommé à la fonction d'attaché le 19 janvier 2024

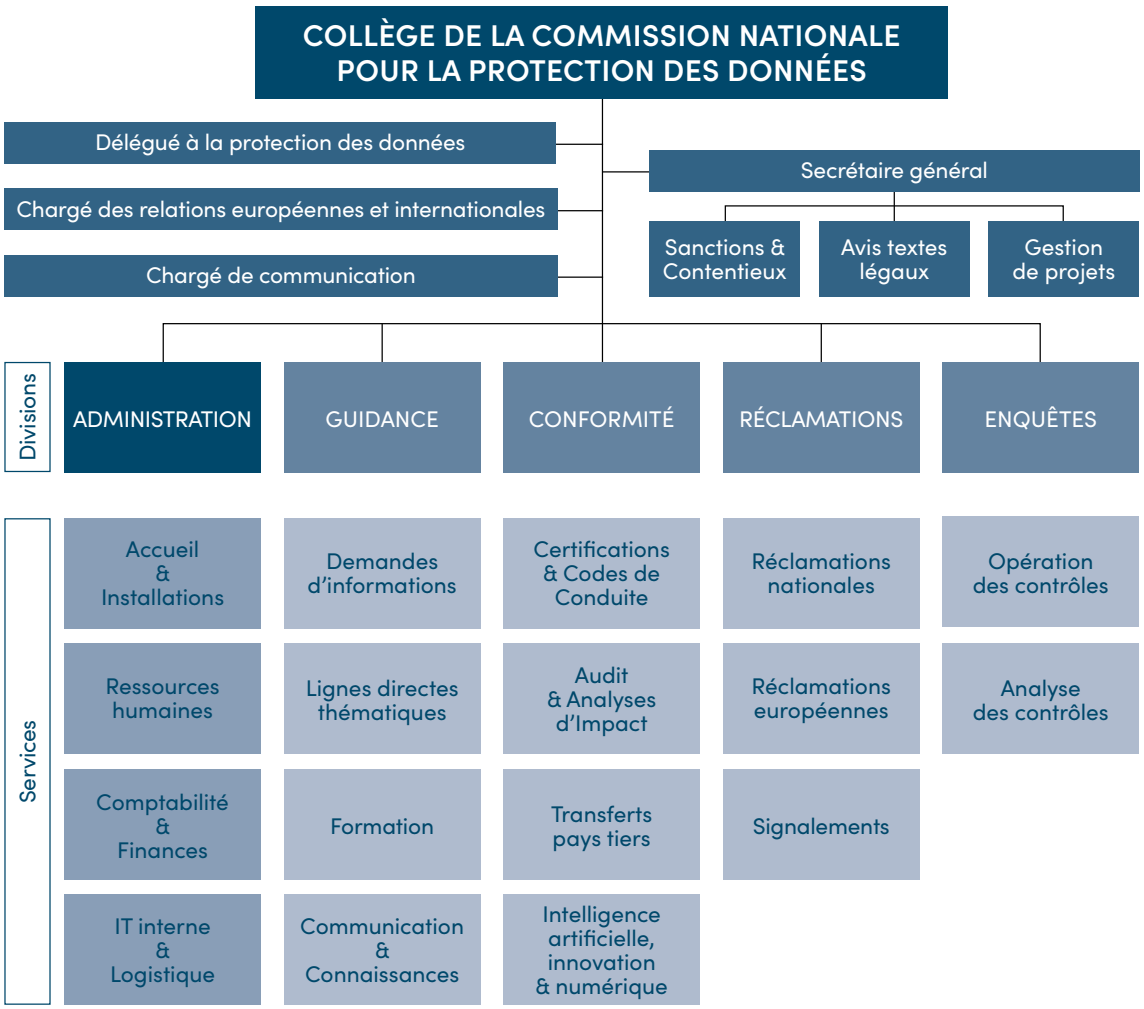
- Madame Nathalie Wangen, nommé à la fonction d'attachée le 19 juillet 2024

- Madame Zoé Becker, nommée à la fonction de rédacteur le 3 septembre 2024

5

2 ORGANISATION DE LA CNPD

L'organigramme ci-dessous (arrêté le 19 avril 2024) donne un aperçu de l'organisation de la CNPD en 2024



RESSOURCES, STRUCTURES ET FONCTIONNEMENT

3 RAPPORT DE GESTION RELATIF AUX COMPTES DE L'EXERCICE 2024

Se situant au milieu de la période de référence visée par son *« Plan stratégique 2023-2025 »* adopté en mars 2023, la Commission nationale pour la protection des données (« CNPD ») s'est concentrée en 2024 sur le développement de ses objectifs stratégiques et opérationnels y visés, tout en assumant les défis auxquels une autorité de surveillance doit faire face dans un monde digital.

Parmi ces défis, il y a lieu de citer notamment l'intégration future dans le fonctionnement actuel de la CNPD des nouveaux textes du paquet numérique adoptés au niveau européen (Data Governance Act, Digital Market Act, Digital Services Act).

De même, suite à l'adoption en date du 13 juin 2024 du règlement européen sur l'intelligence artificielle et la décision subséquente du gouvernement luxembourgeois de désigner la CNPD comme autorité compétente dans ce contexte[7], la définition et l'implémentation des nouvelles missions lui confiées ont été au centre des activités du deuxième semestre de 2024. Ainsi, la CNPD a développé notamment un environnement d'expérimentation de bac à sable (« sandbox ») sur la protection des données dédié à l'intelligence artificielle et permettant de tester en milieu réel, mais fermé et sécurisé, des produits et services par rapport à leur conformité à la réglementation afférente.

Par ailleurs, un des défis repris dans le plan stratégique et ayant entraîné en 2023, tout comme en 2024, une charge de travail considérable, était celui en lien avec le rôle d'autorité de contrôle que la CNPD assure tant au niveau national que dans le contexte des dossiers de réclamation transfrontaliers traités au sein de la coopération européenne et via le mécanisme de coopération et de cohérence du guichet unique.

De plus, et afin d'atteindre les objectifs stratégiques et opérationnels que la CNPD s'est donnée, elle a entamé, entre autres, une série d'actions de sensibilisation prévue dans son programme de travail annuel de 2024. Il s'agissait notamment du déploiement de la campagne de sensibilisation « Droits des citoyens », s'appuyant davantage sur des éléments graphiques, visuels et animés pour faciliter la compréhension auprès des publics non experts. Par ailleurs, la mise en œuvre des séances « Data Protection Basics » a été poursuivie, tout en créant des séances spécifiques permettant de comprendre les défis de l'intelligence artificielle par rapport à la protection des données. Des ateliers de travail (« DaProLab ») sur des sujets divers comme la sécurité des données, les décisions automatisées ou encore le « Privacy by

[7] *cf. projet de loi n° 8476 portant mise en œuvre de certaines dispositions du règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant (...).*

Design » dans le contexte de l'intelligence artificielle ont aussi été organisés.

La CNPD a assisté par ailleurs à une multitude de différents événements, soit en tant que participant, soit en qualité d'intervenant. Au niveau national, il y a lieu de noter par exemple les « Luxembourg Internet Days » organisés par LU-CIX, la Journée internationale des droits de l'Homme ou encore la première édition de « NEXUS2050 », le nouveau salon technologique phare au Luxembourg qui sur deux jours réunissait plus de 5.000 participants. Au niveau européen, la participation à l'atelier européen de traitement des dossiers (« European Case Handling Workshop ») à Tallinn (Estonie), la conférence « RAID » à Bruxelles (Belgique) ou encore le « Privacy Symposium » à Venise (Italie), une conférence internationale destinée à faciliter le dialogue, la coopération et la convergence parmi experts, chercheurs et autorités de protection des données du monde entier, sont à souligner.

Parmi les évènements co-organisés par la CNPD en 2024, la CNPD a contribué à l'organisation de la 2ième édition du « Symposium on Cybersecurity and Data Protection in Humanitarian Action » (Symposium sur la cybersécurité et la protection des données dans le domaine de l'action humanitaire) du Comité International de la Croix-Rouge à Luxembourg-ville. S'y ajoute encore la finalisation du projet ALTO, cofinancé par la Commission européenne, et réalisé ensemble avec la « Luxembourg House of Cybersecurity » et le « National Cybersecurity Competence Center ». Ledit projet a permis le développement d'un outil d'aide à la mise en conformité au RGPD, dénommé DAAZ et répondant aux défis des start-ups et des PME.

Finalement, il y a lieu de relever la participation active de la CNPD aux travaux du Comité européen pour la protection des données, de ses sous-groupes de travail et des task-forces (plus de 170 réunions en 2024), capitale pour répondre aux besoins partagés des autorités et aux questions des citoyens européens, des entreprises multinationales et des PME locales.

Au vu des activités toujours croissantes de la CNPD, activités devenant par ailleurs de plus en plus chronophages, il va sans dire qu'un renforcement du cadre du personnel en 2024 s'est avéré indispensable au bon fonctionnement de l'établissement public. Ainsi, le cadre du personnel a été renforcé par six recrutements supplémentaires d'agents fonctionnaires, respectivement sous contrats à durée indéterminée, épaulés par plusieurs engagements à durée déterminée, dont certains ont été transformés en contrat à durée indéterminée.

Quant au développement futur de ses activités, la CNPD poursuivra sa mission de sensibilisation tout en développant des outils de conformité qu'elle entend promouvoir. De plus, ses activités d'enquête seront intensifiées et ses structures organisationnelles renforcées.

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

LE BUDGET

Le budget de la CNPD s'est élevé pour l'exercice 2024 à un montant de 10 333 489 €, soit une augmentation de 11,56 % par rapport au budget de l'année précédente.

L'augmentation de 1 070 718 € par rapport à 2023 résulte d'un côté de l'évolution des rémunérations du personnel permanent en place au 1er janvier 2024 et d'un autre côté des recrutements de renforcement sollicités et obtenus lors de l'établissement des propositions budgétaires pour l'exercice 2024.

LES DÉPENSES

Au cours de l'exercice 2024, le total des dépenses de l'établissement public s'est élevé à 10 491 338 € par rapport à 9 469 656 € en 2023, soit une progression de 10,79 %.

Cette augmentation résulte principalement des recrutements de renforcement prévus au budget de l'exercice 2024. S'y ajoutent encore les rémunérations des employés engagés sous contrat à durée déterminée dans le cadre des projets ALTO et WTOON, respectivement en vue du remplacement de plusieurs congés de maternité et parentaux.

1. Actif immobilisé

Dans le respect de l'article 46 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données disposant que *« les comptes de la CNPD sont tenus selon les règles de la comptabilité commerciale »*, les dépenses en rapport avec l'acquisition de mobilier, de logiciels et de matériel informatique ont été comptabilisées au bilan de l'établissement public ; leur amortissement étant enregistré parmi les frais de fonctionnement.

Les dépenses en vue de l'acquisition de nouveaux équipements informatiques se sont élevées à 17 516 € par rapport à 58 669 € en 2023. Cette diminution s'explique notamment par le fait qu'en vue du basculement futur vers Windows 11, un grand nombre de laptops ont déjà été remplacés en 2023.

S'y ajoute l'acquisition de mobilier nécessaire pour un montant de 31 439 €, alors qu'en 2023 ce poste ne s'élevait qu'à 12 659 €. Cette augmentation s'explique par la nécessité de réaménager plusieurs bureaux.

2. Frais de fonctionnement

Les frais de fonctionnement au montant de 1 269 431 € ont connu une légère hausse de 4,27 % par rapport à ceux de l'exercice 2023 qui se sont élevés à 1 217 410 €.

2.1. Frais généraux

Représentant 76,38 % des frais généraux, le loyer et les charges locatives au montant total de 743 057 € ont augmenté légèrement par rapport à 2023 où les frais afférents s'élevaient à 710 581 €. Ledit montant se

compose, d'une part, de 632 697 € pour le loyer et de 103 960 € pour les charges locatives du siège de la CNPD (le bâtiment NAOS), et, d'autre part, de 6.400€ pour les charges locatives de son annexe se situant au bâtiment TWIST dans lequel certains agents de la CNPD ont déménagé en octobre 2024 et qui est gratuitement mis à disposition par l'État luxembourgeois qui en est le propriétaire.

S'y ajoutent encore les frais de location de salles de réunion, les frais de stockage externe des archives et la location de plusieurs emplacements de parking au P&R Belval des CFL, le tout pour un montant total de 13 775 € par rapport à 14 432 € en 2023.

En raison d'une baisse des recours en justice introduits en 2024 contre les décisions de la CNPD, les frais d'honoraires juridiques au montant de 74 532 € ont diminué de 45,06 % par rapport à ceux de l'exercice 2023 où les frais en question se sont élevés à 135 669 €.

Les frais de nettoyage des locaux de la CNPD, y compris les produits d'entretien, se sont élevés à 58 953 € par rapport à 54 014 € en 2023.

L'entretien des locaux a occasionné une dépense au montant de 4 438 € par rapport à 4 542 € au cours de l'exercice précédent.

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 13 314 €, 9 578 € et 8 835 € sont restées stables par rapport à 2023 ou elles se sont élevées à 15 259 €, 8 192 € et 9 869 €.

Quant aux frais d'honoraires, ils comprennent, outre les honoraires juridiques mentionnés en amont, les dépenses relatives à la révision des comptes dont les frais se sont élevés à 7 067 € par rapport à 6 838 € en 2023.

Les autres charges générales au montant de 36 089 €, comprenant notamment les frais en rapport avec l'organisation de conférences y compris les frais de représentation, ainsi que les frais d'assurances, d'électricité, d'élimination des déchets et de gardiennage, se chiffrent à respectivement 11 237 €, 15 477 €, 4 106 € et 5 269 €. Les dépenses afférentes ont connu une baisse non négligeable par rapport à 2023 où elles se sont élevées à 51 671 € (28 923 €, 12 900 €, 4 752 € et 5 096 €) en raison notamment de l'organisation d'une conférence sur le Métavers et d'un atelier sur le thème de la certification. S'y ajoutent encore les cotisations à payer à partir de 2024 à diverses associations actives dans le domaine de la protection des données et s'élevant à 3 232 €.

2.2. Communication et relations publiques

Mis à part les frais de communication proprement dits, ce poste comprend en outre les frais de voyage des agents de la CNPD occasionnés essentiellement dans le cadre de leur participation à des réunions du Comité européen pour la protection des données, respectivement de ses sous-groupes

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

de travail et task-forces. Les dépenses y relatives se sont élevées à un montant de 65 850 € pour l'exercice 2024 par rapport à 38 005 € en 2023. Cette hausse de 73,27 % s'explique notamment par la participation à diverses conférences, comme par exemple la « Privacy Symposium Conference » à Venise (Italie) où la CNPD est intervenue lors de dix différents panels, la « Spring Conference » à Riga (Lettonie) ou encore la participation à un groupe de travail sur l'implémentation du règlement européen sur l'intelligence artificielle à Larnaca (Chypre).

Les frais de communication et de publication sont restés quasi identiques (36 797 €) par rapport à 2023 (36 085 €) et comprennent les frais de publication du rapport annuel 2023 s'élevant à 15 385 €, la publication de vacances de postes à raison de 8 151 €, auxquels s'ajoutent divers autres achats de matériel et de services publicitaires au montant de 13 261 €.

Finalement, l'organisation, respectivement la participation financière à l'organisation de différentes conférences ont occasionné des frais s'élevant à un montant de 19 380 € par rapport à 7 014 € en 2023. Cette hausse s'explique notamment par la participation par des expositions ou des stands d'information à divers événements nationaux comme les « Luxembourg Internet Days » ou le nouveau salon technologique « NEXUS2050 ».

2.3. Frais informatiques

Les frais informatiques se sont élevés en 2024 à 174 535 € par rapport à 121 759 € en 2023 et se composent essentiellement de la redevance due 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 se sont élevés à 113 887 € par rapport à 95 115 € en 2023. La croissance de 19,74 % va de pair avec l'évolution du cadre du personnel.

S'y ajoutent encore les frais de location et d'entretien des imprimantes à raison de 11 284 € par rapport à 8 440€ en 2023. Pour ce qui est des frais de maintenance des équipements et des autres frais informatiques, tout comme des frais de développement d'applications informatiques, il est à noter que les dépenses afférentes au montant de 49 364 € ont connu une forte croissance, alors qu'elles s'élevaient à 22 204 € au cours de l'exercice 2023. Cette progression est essentiellement due à des dépenses en relation avec les projets ALTO et WTOON.

3. Frais de personnel

Les rémunérations du personnel se sont élevées en 2024 à 9 127 616 € par rapport à 8 023 320 € en 2023, cette progression étant essentiellement due aux recrutements de renforcement prévus au budget de l'exercice 2024 auxquels s'ajoutent, en outre, les rémunérations des employés engagés sous contrats à durée déterminée non prévues au budget et financées grâce aux réserves constituées au cours des dernières années.

Outre les quatre commissaires, l'effectif total autorisé comprenait au 31 décembre 2024 :

- 54 postes du groupe de traitement ou d'indemnité A1,
- 2 postes du groupe d'indemnité A2 ainsi que
- 6 postes du groupe de traitement ou d'indemnité B1.

Mises à part les rémunérations, les frais de personnel comprennent encore un montant de 22 762 € représentant les dépenses se rapportant à la formation du personnel, soit une augmentation de 6 799 € par rapport à 2023, allant de pair avec l'évolution des effectifs.

4. Autres frais

Il s'agit d'abord des frais engendrés par la voiture de service au montant de 6 513 €, restés stables par rapport à ceux de l'exercice 2023.

Ensuite l'amortissement du mobilier et du matériel informatique comptabilisé pour un montant de 59 974 € suit celui des investissements effectués et présente une légère augmentation par rapport à 53 557 € en 2023 et résultant notamment du remplacement progressif du parc informatique engagé à partir de l'exercice 2023.

S'y ajoutent encore les frais bancaires et charges assimilées au montant de à 895 € par rapport à 575 € de l'année précédente. Finalement, le déménagement de certains agents de la CNPD en octobre 2024 vers le bâtiment TWIST, juste en face du bâtiment NAOS, a occasionné des frais au montant de 4 146 €.

LES RECETTES

Si la CNPD ne dispose pas de recettes au sens propre du terme, elle peut néanmoins et en vertu de l'article 47 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, imposer des redevances dans le cadre de ses pouvoirs d'autorisation et de consultation.

En 2024, une redevance unique de 2 000 € a été imposée. S'y ajoutent les recettes du 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, respectivement au P&R Belval des CFL et s'élevant à 19 380 € par rapport à 14 759 € en 2023.

S'y ajoutent encore les participations de la Commission européenne aux frais se rapportant aux projets ALTO et WTOON pour un montant de 118 013 €. Pour le projet ALTO, la participation s'est élevée à 76 441 € par rapport à 127 307 € pour l'exercice 2023, tandis que le projet WTOON n'a débuté que le 1er novembre 2024 avec une participation de la Commission européenne de 41 572 €.

Le montant de 22 737 € pour produits d'exploitation divers se compose d'un redressement de 16 056 € du loyer NAOS de 2023 et d'un remboursement par une

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

société de leasing de 1 188 €, concernant l'ancienne voiture de service et se rapportant également à l'exercice 2023. S'y ajoute encore la prise en charge par le propriétaire du bâtiment NAOS des frais de stockage temporaire des archives de la CNPD dans le cadre de travaux réalisés au sous-sol du bâtiment et se chiffrant à 5 493 €.

Les intérêts sur comptes bancaires se sont élevés à 95 193 € par rapport à 100 568 € en 2023.

LE RÉSULTAT D'EXPLOITATION

Compte tenu de la dotation annuelle de 10 333 489 € (9 262 771 € en 2023), dont la Commission nationale pour la protection des données a bénéficié de la part de l'État en application de l'article 47 de la loi du 1er août 2018 précitée, le résultat d'exploitation positif de l'établissement public s'élève au 31 décembre 2024 à 99 474 € par rapport à 35 749 € en 2023.

5

ANNEXES

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

120

- Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal concernant la coopération interadministrative entre le Ministère de la Mobilité et des Travaux publics et l'Administration de l'enregistrement, des domaines et de la TVA (Délibération n° 1/AV1/2024 du 19 janvier 2024)

123

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8309 portant mise en œuvre du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) et portant modification de : 1° la loi modifiée du 14 août 2000 sur le commerce électronique ; 2° la loi modifiée du 30 novembre 2022 relative à la concurrence (Délibération n°3/AV2/2024 du 19 janvier 2024)

131

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8180 fixant les conditions relatives à l'organisation des transports sanitaires terrestres non urgents (Délibération n°8/AV3/2024 du 23 février 2024)

137

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8331 portant modification de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique et relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du carnet de vaccination électronique (Délibération n°9/AV4/2024 du 23 février 2024)

150

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8250 concernant le comptage divisionnaire et la répartition des coûts de chaleur, de froid et d'eau chaude sanitaire et au projet de règlement grand-ducal concernant le comptage divisionnaire et la répartition des coûts de chaleur, froid et eau chaude sanitaire et modifiant le 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 (Délibération n°10/AV5/2024 du 23 février 2024)

159

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8355 portant modification 1° de la loi électorale modifiée du 18 février 2003 et 2° de la loi modifiée du 16 juin 2017 sur l'organisation du Conseil d'État (Délibération n°16/AV6/2024 du 8 mars 2024)

164

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8305 portant : 1° mise en œuvre du règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n°1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission ; 2° mise en œuvre du règlement (UE) 2022/1190 du Parlement européen et du Conseil du 6 juillet 2022 modifiant le règlement (UE) 2018/1862 en ce qui concerne l'introduction dans le système d'information Schengen (SIS) de signalements pour information concernant des ressortissants de pays tiers dans l'intérêt de l'Union ; 3° mise en œuvre de l'article 20 du règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 ; 4° mise en œuvre de l'article 20 du règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n°767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil ; 5° modification du Code de procédure pénale ; 6° modification du Code civil ; 7° modification de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ; 8° modification de la loi modifiée du 18 décembre 2015 relative à la protection internationale et à la protection temporaire ; 9° modification de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 10°modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale (Délibération n° 17/AV7/2024 du 15 mars 2024

ANNEXES

176
- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8253 relative aux fiches d'hébergement et portant : 1° modification de loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 2° modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ; et 3° abrogation de la loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement (Délibération n°20/AV8/2024 du 29 mars 2024)

188
- Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal relatif à la plateforme de données énergétiques (Délibération n°21/AV9/2024 du 26 avril 2024)

198
- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8335 relative à la sécurité, la sûreté, l'ordre et la vidéosurveillance dans les transports publics et modifiant la loi du 5 février 2021 sur les transports publics (Délibération n°25/AV10/2024 du 2 mai 2024)

214
- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8216 relative au droit de préemption en faveur de la promotion de l'habitat et modifiant 1° la loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu ; 2° loi modifiée du 22 octobre 2008 sur le droit d'emphytéose et le droit de superficie et introduisant différentes mesures administratives et fiscales en faveur de la promotion de l'habitat (Délibération n°26/AV11/2024 du 2 mai 2024)

219
- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8148 relative à la rétention des données à caractère personnel et portant modification : 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État (Délibération n°28/AV12/2024 du 16 mai 2024)

261
- Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°7961 modifiant 1° la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises ; 2° la loi modifiée du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs

(Délibération n°29/AV13/2024
du 16 mai 2024)

264

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8193 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale
(Délibération n°30/AV/14/2024
du 16 mai 2024)

270

- Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°7994 portant aide, soutien et protection aux mineurs, aux jeunes adultes et aux familles portant modification : 1. du Code du travail ; 2. du Code de la sécurité sociale ; 3. de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ; 4. de la loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'État ; 5. de la loi modifiée du 4 juillet 2008 sur la jeunesse ; 6. de la loi modifiée du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 7. de la loi du 1er août 2019 concernant l'institut étatique d'aide à l'enfance et à la jeunesse ; et portant abrogation 1. de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse ; 2. de la loi modifiée du 16 décembre 2008 relative à l'aide à l'enfance et à la famille
(Délibération n°31/AV15/2024
du 16 mai 2024)

278

- Avis de la Commission nationale pour la protection des données relatif 1. au projet de loi n°8232 relatif à l'autopartage sur la voie publique et portant modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques ; 2. au projet de règlement grand-ducal portant réglementation de l'autopartage sur la voie publique et portant modification : 1° de l'arrêté grand-ducal modifié du 23 novembre 1955 portant règlement de la circulation sur toutes les voies publiques ; 2° du règlement grand-ducal modifié du 26 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 ; 3° du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers
(Délibération n°39/AV16/2024
du 21 juin 2024)

285

- Avis de la Commission nationale pour la protection des données relatif aux amendements gouvernementaux sur le projet de loi n°7511 relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances
(Délibération n°44/AV17/2024
du 28 juin 2024)

ANNEXES

288

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8089 relatif à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique et au projet de règlement grand-ducal fixant certaines modalités d'application de la loi relative à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique (Délibération n°45/AV18/2024 du 4 juillet 2024)

299

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8330B portant organisation de l'Administration du cadastre et de la topographie et au projet règlement grand-ducal concernant la consultation et la diffusion de la documentation relative à la mensuration officielle, de la documentation cadastrale, de la documentation topographique, du registre national des localités et des rues et des systèmes de référence de coordonnées nationaux gérés par l'Administration d cadastre et de la topographie ; et portant fixation du tarif des redevances 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 (Délibération n°51/AV19/2024 du 7 août 2024)

307

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8082 sur l'impôt foncier, l'impôt à la mobilisation de terrains et l'impôt sur la non-occupation de logements, modifiant 1° la loi modifiée dite « Abgabenordnung (AO) » du 22 mai 1931 ; 2° la loi modifiée dite « Bewertungsgesetz (BewG) » du 16 octobre 1934 ; 3° la loi modifiée dite « Steueranpassungsgesetz (StAnpG) » du 16 octobre 1934 ; 4° la loi modifiée du 17 avril 1964 portant réorganisation de l'administration des contributions directes ; 5° la loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu ; 6° la loi modifiée du 30 avril 2004 autorisant le Fonds national de solidarité à participer aux prix des prestations fournies dans le cadre de l'accueil aux personnes admises dans un centre intégré pour personnes âgées, une maison de soins ou un autre établissement médico-social assurant un accueil de jour et de nuit ; 7° la loi modifiée du 19 juillet 2004 concernant l'aménagement communal et le développement urbain ; 8° la loi modifiée du 22 octobre 2008 sur le droit d'emphytéose et le droit de superficie et introduisant différentes mesures administratives et fiscales en faveur de la promotion de l'habitat ; 9° la loi modifiée du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement ; 10° la loi du 28 juillet 2018 relative au revenu d'inclusion sociale ; 11° la loi du 22 juillet 2022 relative à une subvention de loyer et abrogeant :

1° la loi modifiée du 19 juillet 1904 sur les impositions communales ; 2° la loi modifiée dite « Grundsteuergesetz (GrStG) » du 1er décembre 1936
(Délibération n°52/AV20/2024 du 7 août 2024)

325

- Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 8186A portant modification de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; de la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes, des droits d'accise sur l'eau-de-vie et des cotisations d'assurance sociale ; de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines, de l'Administration des douanes et accises et portant modification de la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée; la loi générale des impôts (« Abgabenordnung ») ; la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes; la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines ; la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale
(Délibération n°53/AV21/2024 du 7 août 2024)

337

- Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°7650 portant modification 1° du Code de la consommation ; 2° de la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des spécialités pharmaceutiques et des médicaments préfabriqués ; 3° de la loi modifiée du 27 juillet 1991 sur les médias électroniques ; 4° de la loi modifiée du 27 juillet 1997 sur le contrat d'assurance ; 5° de la loi modifiée du 14 août 2000 relative au commerce électronique ; 6° de la loi modifiée du 24 mai 2011 relative aux services dans le marché intérieur ; 7° de la loi modifiée du 23 décembre 2016 sur les ventes en soldes et sur trottoir et la publicité trompeuse et comparative ; 8° de la loi du 26 juin 2019 relative à certaines modalités d'application et à la sanction du règlement (UE) 2018/302 du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n°2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE, en vue de la transposition de la directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE

ANNEXES

(Délibération n°54/AV22/2024
du 16 août 2024)

345
- Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal relatif à la plateforme de données énergétiques
(Délibération n°55/AV23/2024
du 23 août 2024)

347
- Avis complémentaire de la Commission nationale pour la protection des données relatif au 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'État
(Délibération n°56/AV24/2024
du 30 août 2024)

352
- Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal portant modification du règlement grand-ducal du 22 janvier 2009 concernant la coopération interadministrative de l'Administration des Contributions Directes et de l'Administration de l'enregistrement et des Domaines
(Délibération n°57/AV25/2024
du 30 août 2024)

356
- Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif au 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'État
(Délibération n°60/AV26/2024
du 31 octobre 2024)

361
- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8421 sur la promotion du journalisme professionnel et du débat démocratique, portant modification : 1° de la loi modifiée du 8 juin 2004 sur la liberté d'expression dans les médias ; 2° de la loi modifiée du 14 septembre 2018 relative à une administration transparente et ouverte ; 3° de la loi du 30 juillet 2021 relative à un régime d'aides en faveur du journalisme professionnel
(Délibération n°63/AV27/2024
du 7 novembre 2024)

365
- Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8317 relative à la transition énergétique et modifiant : 1° la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité ; et 2° la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz nature

(Délibération n°68/AV28/2024
du 15 novembre 2024)

383

- Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°8186A portant modification de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; de la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes, des droits d'accise sur l'eau-de-vie et des cotisations d'assurance sociale ; de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines, de l'Administration des douanes et accises et portant modification de la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée; la loi générale des impôts (« Abgabenordnung ») ; la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes ; la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines ; la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale
(Délibération n°69/AV29/2024
du 22 novembre 2024)

385

- Avis complémentaire de la Commission nationale pour la protection des données relatif au projet n°8253 relative aux fiches d'hébergement et portant : 1° modification de loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 2° modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ; et 3° abrogation de la loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement
(Délibération n°70/AV30/2024
du 6 décembre 2024)

392

- Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal portant exécution de l'alinéa 2 du paragraphe 22bis de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung »)
(Délibération n°71/AV31/2024
du 13 décembre 2024)

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal concernant la coopération interadministrative entre le Ministère de la Mobilité et des Travaux publics et l'Administration de l'enregistrement, des domaines et de la TVA

Délibération n°1/AV1/2024
du 19 janvier 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 »*.

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

2. Par courrier reçu le 9 octobre 2023, le Ministère des Finances a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal concernant la coopération interadministrative entre le Ministère de la Mobilité et des Travaux publics et l'Administration de l'enregistrement, des domaines et de la TVA (ci-après le « projet de règlement grand-ducal »).

3. Selon l'exposé des motifs, le projet de règlement grand-ducal porte exécution de l'article 14.2 de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines et de l'Administration des douanes et accises et portant modification de - la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée ; la loi générale des impôts (« Abgabenordnung ») ;
- la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes ; - la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines ; - la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale (ci-après la « loi modifiée du 19 décembre 2008 »).

4. Le second paragraphe de l'article 14 fut inséré dans la loi modifiée du 19 décembre 2008 par une loi du 20 juillet 2022 qui a

fait l'objet de deux avis de la CNPD[1]. Cette disposition concerne la transmission par le Ministère des Transports d'informations sur les véhicules immatriculés à l'Administration de l'enregistrement, des domaines et de la TVA (ci-après l' « AED ») en vue de la vérification de l'exacte perception de la TVA. Conformément à l'alinéa 2 de l'article 14.2 précité, le projet de règlement grand-ducal entend préciser les modalités de la communication des données entre le Ministère des Transports et l'AED.

I. Quant l'article 1.1 du projet de règlement grand-ducal

5. La seule précision apportée par l'article 1.1 du projet de règlement grand-ducal par rapport à l'article 14.2 de la loi modifiée du 19 décembre 2008 est que la transmission des données s'effectue *« par le biais d'un système informatique »*.

6. Dans son avis du 12 décembre 2023, le Conseil d'État propose de compléter ce libellé par les termes *« sécurisé moyennant une authentification forte »*. Cette proposition du Conseil d'État rejoint les observations formulées par la CNPD dans son avis 4 mars 2022[2] relatif au projet de loi n°7872 qui allait devenir la loi du 20 juillet 2022. Dans ledit avis, la CNPD soulignait notamment l'importance de garantir une sécurité appropriée des données personnelles, conformément aux articles 5.1.f) et 32 du RGPD.

II. Quant à l'article 1.2 du projet de règlement grand-ducal

7. La CNPD note une certaine incohérence dans la terminologie employée dans le projet de règlement grand-ducal, créant des incertitudes quant aux modalités pratiques de la mise à disposition des données. Ainsi, l'article 1.2 du projet de règlement grand-ducal évoque un « accès de l'[AED] aux informations stockées dans les bases de données électroniques visées au paragraphe 1er », tandis que l'article 1.1 du projet de règlement grand-ducal, tout comme l'article 14.2 de la loi modifiée du 19 décembre 2008, prévoit qu'il appartient au Ministère des Transports de transmettre à l'AED les données énumérées aux points 1° et 2° de l'article 14.2 précité.

8. L'article 1.2 du projet de règlement grand-ducal, en ce qu'il semble prévoir un accès direct de l'AED aux données détenues par le Ministère des Transports, risque de ne pas être conforme à la loi modifiée du 19 décembre 2008 qui, quant à elle, ne prévoit qu'une transmission de données. Par ailleurs, il est fait référence à des « bases de données électroniques visées au paragraphe 1er » alors que le paragraphe 1er ne mentionne pas de telles bases de données mais ne fait que renvoyer aux données énumérées à l'article 14.2 de la loi modifiée du 19 décembre 2008.

9. La Commission nationale note favorablement que l'article 1.2 du projet

[1] Délibération n°2/AV2/2022 du 4 mars 2022 de la Commission nationale pour la protection des données, doc. parl. n°7872/05 ; Délibération n°16/AV8/2022 du 13 mai 2022 de la Commission nationale pour la protection des données, doc. parl. n°7872/07.
[1] Délibération n°2/AV2/2022 du 4 mars 2022 de la Commission nationale pour la protection des données, doc. parl. n°7872/05, p. 8.

ANNEXES

de règlement grand-ducal précise limitativement les catégories de personnes ayant le droit d'accéder à ces données. En effet, en vertu du principe de sécurité et de confidentialité consacré aux articles 5.1.f) et 32 du RGPD, seules les personnes habilitées devraient avoir accès aux données dont elles ont besoin dans le cadre de leurs activités. Il est toutefois à regretter que le projet de règlement grand-ducal ne prévoie pas de système de journalisation des accès, tel que suggéré par la CNPD dans son avis du 4 mars 2022[3].

Ainsi adopté à Belvaux
en date du 19 janvier 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[3] Délibération n°2/AV2/2022 du 4 mars 2022 de la Commission nationale pour la protection des données, doc. parl. n° 7872/05, p. 8.

6

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8309 portant mise en œuvre du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) et portant modification de : 1° la loi modifiée du 14 août 2000 sur le commerce électronique ; 2° la loi modifiée du 30 novembre 2022 relative à la concurrence

Délibération n°3/AV2/2024
du 19 janvier 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 Monsieur le Ministre de l'Economie, 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°8309 portant mise en œuvre du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) et portant modification de : 1° la loi modifiée du 14 août 2000 sur le commerce électronique ; 2° la loi modifiée du 30 novembre 2022 relative à la concurrence.

2. Le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre et modifiant la directive 2000/31/CE du Parlement européen et du Conseil relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (ci-après le « règlement » ou le « DSA ») vise à moderniser certaines législations nationales relatives au secteur numérique. Ce faisant, le règlement et le projet de loi y afférant viennent impacter d'importantes notions relatives à la protection des données. Dans ce contexte, la CNPD tient à faire part de ses observations par rapport à certains articles du projet de loi et du règlement présentant des aspects ayant trait à la protection des données à caractère personnel.

3. Le présent avis n'examine pas en détail le projet de loi mais se limitera à soulever les problématiques fondamentales qui se posent au regard de la protection des données. Pour une analyse plus approfondie du DSA,

ANNEXES

il est renvoyé à l'avis 1/2021 du contrôleur européen de la protection des données (ci-après l'« EDPS ») du 10 février 2021[4].

I. Concernant l'article 23 du projet de loi

4. La CNPD exprime son inquiétude quant à la rédaction actuelle des articles 23.1 et 23.2 du projet de loi en ce qu'ils permettent à l'Autorité de la concurrence de prendre des décisions relatives à la protection des données personnelles : « Si l'administration centrale ou l'établissement public consulté n'émet pas d'avis dans le délai imparti, cela n'empêche pas l'Autorité de poursuivre son enquête et d'adopter une décision conformément à la présente loi ». La rédaction de cet article ne retranscrit pas, d'une part le considérant 109 du DSA qui dispose que : *« Le présent règlement n'impose pas aux États membres de confier aux autorités compétentes la mission de se prononcer sur la licéité d'éléments de contenus spécifiques. » et d'autre part, la volonté des rédacteurs du projet de loi qui précisent dans leurs propos liminaires : « Il est important de noter ici que le DSC sera chargé de contrôler et chapeauter la mise en œuvre du DSA, sans pour autant toucher aux compétences des autorités sectorielles déjà en place. Une délimitation doit être faite entre, d'un côté, la réglementation du contenu-même sur internet – traitée par les textes sectoriels – et, de l'autre côté, la coordination des procédures prévues par le DSA, qui est propre au DSC. En effet, le DSA ne confie pas au DSC la mission de se prononcer sur la licéité d'éléments de contenus spécifiques – compétence exclusive relevant des différentes autorités sectorielles. »*. La CNPD insiste sur le fait qu'en l'état actuel de la rédaction de l'article 23, la saisine par l'Autorité de la concurrence des autorités sectorielles est facultative, ce qui ne permet, ni d'assurer une protection adéquate de la vie privée et des libertés fondamentales, ni de garantir le principe de sécurité juridique concernant les points évoqués. La Commission nationale estime opportun pour les rédacteurs du projet de loi de revoir la rédaction dudit article afin de trouver un juste équilibre entre le principe de coopération loyale[5] et l'indépendance des différentes autorités.

5. Par ailleurs, l'article 23 ne présente aucune précision quant au « délai imparti » et les modalités de fixation de ce dernier, en conséquence de quoi la CNPD craint, en l'état de la rédaction actuel du texte, de voir menacée son indépendance par la perte de son autonomie concernant son agenda et ses ressources. En effet, tout dossier présenté par l'Autorité de la concurrence se verra traité prioritairement par la CNPD afin d'éviter toute ingérence concernant sa jurisprudence relative au RGPD. Ce fonctionnement impliquera un détournement des agents au profit de l'Autorité de la concurrence pendant une durée qui échappera à tout contrôle de la Commission nationale. Cette perte d'autonomie pourrait se révéler préjudiciable pour le citoyen qui s'attend à ce qu'une autorité indépendante de défense des libertés fondamentales soit totalement autonome dans sa gestion et

[4] Opinion 1/2021 on the Proposal for a Digital Services Act : https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf

[5] Cour de justice de l'Union européenne Meta v Bundeskartellamt C 252/21

puisse exécuter ses missions en toute liberté et indépendance.

6. D'autre part, la CNPD se préoccupe des conséquences d'une application stricte du texte tel que proposé et plus particulièrement en son premier paragraphe *« [...] A cette fin, l'Autorité peut accéder dans les meilleurs délais à tout document et élément d'information détenus par l'administration centrale ou établissement public concernés utiles à l'accomplissement de sa mission »*, la rédaction telle que proposée ne connait pas de limite dans son application et peut cibler l'entièreté des informations détenues par la Commission nationale. A ce titre, la CNPD se questionne sur les possibles implications de cet article au regard de son indépendance et de sa gestion conformément à l'article 52 du RGPD, ainsi que des conséquences d'une telle disposition compte tenu de la rédaction du paragraphe (2) de l'article 23 du projet de loi. En effet, la saisine des autorités sectorielles n'étant pas imposée par la rédaction actuelle du projet de loi, la CNPD craint qu'il ne soit loisible pour l'Autorité de la concurrence, une fois en possession de l'ensemble des documents détenus par la CNPD, d'interpréter ces documents et informations qui aurait été fournis ultérieurement sur base du paragraphe (1), et ainsi, de prendre des décisions relatives à la protection des données sans avoir précédemment sollicité la Commission nationale ou en privant celle-ci d'un délai raisonnable pour formuler son avis. La CNPD constate au surplus que les rédacteurs du projet de loi s'expriment en ce sens dans le commentaire des articles : *« Dans ce cas [non-respect du délai], l'Autorité peut poursuivre son enquête et adopter, le cas échéant, une décision sur la base des informations disponibles et des avis exprimés par d'autres administrations publiques, ou en se basant sur son propre jugement d'expert ».* La CNPD souhaiterait donc voir restreint l'accès à ses documents et informations aux situations précisées par la jurisprudence de la Cour de justice de l'Union européenne[6] et notamment dans les cas où l'Autorité de la concurrence nourrirait des doutes concernant : *« La portée de l'appréciation effectuée par la [CNPD] ou l'autorité de contrôle chef de file, lorsque le comportement en cause ou un comportement similaire fait, en même temps, l'objet d'un examen de la part de ces autorités, ou encore lorsque, en l'absence d'enquête desdites autorités, elle considère qu'un comportement d'une entreprise n'est pas conforme aux dispositions du RGPD »*

7. En outre, la CNPD se félicite de l'intention des rédacteurs d'instaurer un groupe de travail afin, comme le précise ces derniers dans l'exposé des motifs du projet de loi : *« d'assurer une bonne application du DSA »*. Toutefois, la Commission nationale souhaiterait attirer l'attention sur le fait que les rédacteurs du projet de loi n'ont pas expressément envisagé, dans la rédaction actuelle du projet de loi, la structure, les ressources et le fonctionnement du groupe de travail. Il pourrait en effet se révéler opportun de déterminer les participants d'un tel groupe, son budget de fonctionnement, et ses objectifs à court, moyen et long terme. La CNPD considère que l'encadrement légal d'un tel groupe garantirait une application

[6] Cour de justice de l'Union européenne Meta v Bundeskartellamt C 252/21

ANNEXES

saine du DSA et un respect des différentes compétences octroyées aux diverses autorités sectorielles qui d'ailleurs ne sont pas définies dans le projet de loi. En outre, la CNPD tient à préciser que cette exigence de coopération a été appréciée par la Cour de justice de l'Union européenne à travers une jurisprudence constante : *« Ainsi, compte tenu de ce principe [de coopération loyale], lorsque les autorités de la concurrence nationales sont amenées, dans l'exercice de leurs compétences, à examiner la conformité d'un comportement d'une entreprise aux dispositions du RGPD, elles doivent se concerter et coopérer loyalement avec les autorités de contrôle nationales concernées ou avec l'autorité de contrôle chef de file, l'ensemble de ces autorités étant alors tenues, dans ce contexte, de respecter leurs pouvoirs et compétences respectifs, de manière à ce que les obligations découlant du RGPD ainsi que les objectifs de ce règlement soient respectés et que leur effet utile soit préservé »*[7]. Dans ce contexte la Commission nationale regrette que les rédacteurs du projet de loi n'aient pas choisi d'aller plus loin dans l'encadrement de ladite coopération.

8. Pour les raisons exprimées ci-dessus et en vertu du principe de sécurité juridique, la Commission nationale estime nécessaire, d'une part, que l'accès à ses documents et informations doit être limité à ce que la Commission nationale estime comme nécessaire pour la raison qui lui est présentée, et, d'autre part, que les auteurs du projet de loi octroient à la CNPD des compétences dans le contexte des articles présentant une inférence significative avec le RGPD tel que listé ci-après.

II. <u>Sur l'opportunité de désigner la CNPD comme autorité compétente pour certains articles du DSA</u>

9. Selon l'exposé des motifs du projet de loi, la désignation de l'Autorité de la concurrence en tant que coordinateur pour les services numériques vise à mettre en œuvre l'article 49 du DSA. S'il est bien précisé que l'article 49 laisse à l'État membre la possibilité de désigner plusieurs autorités compétentes, comme cela est concrètement envisagé par la France[8], la Lituanie[9] et la Finlande[10], l'exposé des motifs reste silencieux sur les raisons qui ont amené les rédacteurs du projet de loi à ne pas prévoir une désignation de la CNPD comme autorité compétente. A ce titre, et au regard des inférences potentielles du projet de loi avec l'application du RGPD, la Commission nationale tient à faire part de ses observations compte tenu de certains articles du DSA et du projet de loi, qui, s'ils relevaient de sa compétence, permettrait une meilleure application du RGPD et du DSA.

10. Sur la base des éléments suivants, la CNPD souhaiterait que les rédacteurs du projet de loi apprécient l'opportunité d'attribuer compétence à l'autorité pour la protection des données concernant certains articles spécifiques du DSA :

[7] Voir en ce sens arrêts du 14 novembre 1989, (14/88, EU:C:1989:421, point 20), et du 11 juin 1991, (C 251/89, EU:C:1991:242, point 57).
[8] Projet de loi français : https://www.senat.fr/leg/pjl22-593.html
[9] Projet de loi lituanien : https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/35b2f692fe1611edbc0bd16e3a4d3b97
[10] Projet de loi finlandais : https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=861bdfd6-8f38-409a-8f5b-91e08b98c072

6

1. L'article 25 du DSA

11. L'article 25 vise à réguler l'utilisation des *« dark patterns »* ou encore des « deceptive designs » par les fournisseurs de plateformes en ligne. S'il reste opportun pour les différentes autorités sectorielles d'affiner une définition précise des termes « dark patterns » et « deceptive designs », la CNPD a considéré jusqu'à présent comme tel *« des pratiques de design trompeur et des pratiques visant à piéger l'utilisateur »*[11]. Dans ce contexte, la CNPD attire l'attention des rédacteurs du projet de loi sur le fait que ledit article exclut expressément de son champ d'application les pratiques couvertes par le RGPD et la directive 2005/29/CE. Toutefois, la Commission nationale précise qu'une définition uniforme de la notion de *« dark patterns »* devrait être adoptée par les autorités sectorielles luxembourgeoises afin d'assurer une sécurité juridique optimale et un respect des libertés fondamentales. Dans ce contexte la CNPD précise qu'elle a eu l'occasion, via les groupes de travaux européens, de produire des lignes directrices concernant ce domaine spécifique[12]. En tout état de cause, l'application de cet article implique une action coordonnée des autorités sectorielles luxembourgeoises concernées, afin de déterminer les contours des compétences de chaque autorité, par conséquent, la CNPD souhaiterait que le projet de loi sous examen établisse un cadre de coopération renforcé entre les différentes autorités, en ayant, par exemple, recours au groupe de travail que les rédacteurs souhaitent instaurer. A ce titre, la CNPD considère qu'il serait opportun de voir précisé par les rédacteurs du projet de loi une stricte délimitation des champs de compétence concernant le contrôle des *« dark patterns »*. Cette stricte délimitation pourrait se faire, par exemple, par l'élaboration au sein du projet de loi, d'une définition des termes *« dark patterns »* et *« deceptive designs »* au regard du DSA et du RGPD. Une seconde option serait, d'inscrire la rédaction d'une telle définition comme l'un des objectifs du groupe de travail souhaité par les rédacteurs du projet de loi. De cette manière, la CNPD et l'Autorité de la concurrence seraient à même de sanctionner clairement et efficacement des pratiques relevant de leurs compétences respectives.

2. L'article 26 du DSA

12. L'article 26, qui encadre les publicités sur les plateformes en ligne, est fortement lié au RGPD en ce que, d'une part, l'article 26.3 vient interdire la publicité personnalisée basée sur le profilage de données sensibles telles que définies à l'article 9 du RGPD, et, en ce que d'autre part, l'article 26.1.d) du DSA vient déterminer les informations et les moyens de contrôles dont devra disposer le destinataire d'une publicité.

13. Par ailleurs, la CNPD tient à faire observer que le législateur finlandais[13] envisage d'octroyer compétence sur l'article

[11] Lignes directrices en matière de cookies et autres traceurs – CNPD Version du 03.01.2022
[12] Lignes directrices 03/2022 concernant les « modèles de conception trompeuse » ou *« dark patterns/deceptive design »* dans les interfaces des plateformes de médias sociaux : comment les reconnaître et les éviter *(traduction libre) – "Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them"*
[13] Projet de loi finlandais : https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=861bdfd6-8f38-409a-8f5b-91e08b98c072

ANNEXES

26.1.a). b). c) et d) du DSA à son autorité de protection des données, dans les situations où la publicité utilisée n'a pas un objectif commercial. Ce faisant, le législateur finlandais poursuit un travail d'efficience en matière de protection des données personnelles et de la vie privée.

14. En outre, il semble opportun de faire remarquer que la CNIL, l'autorité de protection des données française, s'est vu octroyer, dans un souci de cohérence et de bonne application du RGPD, compétence concernant les articles 26.1.d) et 26.3 du DSA. Cette attribution de compétence revêt une certaine efficacité comme le fait remarquer ladite autorité de protection des données : *« la CNIL estime que cette nouvelle attribution de compétences est logique dans la mesure où ces dispositions ne font que renforcer, pour les fournisseurs de plateformes en ligne, certaines obligations précises issues du RGPD. La correcte application des dispositions des articles 26 (« publicité sur les plateformes en ligne »), 27 (« transparence du système de recommandation ») et 28 (« protection des mineurs en ligne ») du DSA, qui renvoient de manière plus ou moins directe à des enjeux liés à la protection des données, nécessitera une coordination entre les autorités compétentes désignées [...] »*[14].

15. En tout état de cause, la CNPD propose qu'elle soit désignée comme autorité compétente pour l'ensemble des dispositions relatives à l'article 26.3 ainsi que l'article 26.1. b). c). d) du DSA.

3. L'article 27 du DSA

16. L'article 27 *« Transparence du système de recommandation »* vise à permettre à un destinataire d'une publicité (p.ex. un utilisateur d'un réseau social, qui est lui-même souvent une *« personne concernée »* au regard du RGPD) de comprendre pourquoi une publicité le vise en particulier et sur la base de quelles informations. L'article précise que les destinataires des publicités devront se voir expliquer en des termes simples et compréhensibles les moyens dont ils disposent pour modifier ou influencer les paramètres en question. La CNPD constate donc que cet article a pour objectif d'expliquer aux utilisateurs le fonctionnement du profilage, ainsi que de détailler la valeur de chaque donnée personnelle utilisée par le système de recommandation.

17. Dans la mesure où cet article se base sur la notion de profilage et que celui-ci repose sur les données personnelles des utilisateurs, la CNPD estime qu'il revient à l'autorité de la protection des données personnelles de s'assurer que toute transparence soit faite aux personnes concernées et aux utilisateurs sur l'utilisation qui est faite de leurs données. La CNPD rappelle, à l'appui de ses propos, que le Comité européen de la protection des données (CEPD) a déjà eu l'occasion de se prononcer sur le profilage à travers la publication de lignes directrices[15] et qu'en

[14] Délibération n° 2023-036 du 20 avril 2023 portant avis sur le projet de loi « visant à sécuriser et réguler l'espace numérique » : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000047551574?init=true&page=1&query=*&searchField=ALL&tab_selection=cnil

[15] Sans produire une liste exhaustive : EDPB : *« Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 ».*

conséquence il s'agit d'un sujet sur lequel la CNPD possède une certaine expertise.

18. Par ailleurs, le principe selon lequel l'information doit être compréhensible et facilement accessible et qui est précisé en ces termes par l'article 27 du DSA :« Les fournisseurs de plateformes en ligne qui utilisent des systèmes de recommandation établissent dans leurs conditions générales, dans un langage simple et compréhensible » est une récurrence au sein de la protection des données. Par conséquent, la CNPD dispose déjà des compétences et de l'expérience lui permettant d'assurer le respect de cette disposition.

19. En tout état de cause, la CNPD recommande aux rédacteurs du projet de loi de lui octroyer entière compétence sur l'article 27 du DSA.

4. L'article 28 du DSA

20. L'article 28.1 impose aux fournisseurs de plateformes en ligne de mettre *« en place des mesures appropriées et proportionnées pour garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs sur leur service. »*. Ce même article prohibe en son paragraphe 2 aux fournisseurs de plateformes en ligne d'utiliser un système de profilage en *« utilisant des données à caractère personnel concernant le destinataire du service dès lors qu'ils ont connaissance avec une certitude raisonnable que le destinataire du service est un mineur »*. La CNPD considère détenir les compétences et l'expertise nécessaires afin d'assurer le contrôle du respect de cet article, en effet, celle-ci constate que cette obligation présente des similarités importantes avec l'objectif décrit par le considérant 38 du RGPD[16] : *« Cette protection spécifique (celle octroyée aux enfants) devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. »* Elle précise, au surplus, qu'une protection particulière des mineurs est déjà garantie par le RGPD en son article 8 *« Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information »* et que l'article 40.2.g) du RGPD octroie à l'autorité de protection des données la possibilité d'encourager la création de codes de conduite concernant *« les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l' enfant; »*. En outre, la CNPD rappelle qu'elle dispose d'une expérience non négligeable en matière de profilage et de traçage des utilisateurs, par conséquent la Commission nationale s'estime compétente pour assurer le respect de l'article 28.2 du DSA.

21. Enfin, la CNPD ayant déjà compétence pour apprécier l'opportunité d'un traitement de données personnelles il serait opportun de lui attribuer la charge de faire respecter l'article 28.3 du DSA qui précise *« Le respect*

[16] Ainsi qu'au surplus les considérants 58, 65 et 71.

ANNEXES

des obligations énoncées dans le présent article n'impose pas aux fournisseurs de plateformes en ligne de traiter des données à caractère personnel supplémentaires afin de déterminer si le destinataire du service est un mineur. »

22. Par conséquent, la CNPD recommande aux rédacteurs du projet de loi de la désigner compétente pour l'entièreté de l'article 28 du DSA.

Ainsi adopté à Belvaux
en date du 19 janvier 2024

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

6

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8180 fixant les conditions relatives à l'organisation des transports sanitaires terrestres non urgents

Délibération n°8/AV3/2024
du 23 février 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 »*.

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

2. Par courrier reçu le 22 mars 2023, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur le projet de loi n°8180 fixant les conditions relatives à l'organisation des transports sanitaires terrestres non urgents (ci-après le « projet de loi »).

3. Selon l'exposé des motifs, l'objectif principal du projet de loi est d'établir un cadre légal pour les entreprises prestataires de services de transports sanitaires terrestres non urgents, en dehors des missions dévolues au Corps grand-ducal d'incendie et de secours (CGDIS). Ce cadre vise à définir des normes minimales en matière d'équipement et d'hygiène des véhicules, ainsi que les formations nécessaires du personnel. À cette fin, la loi en projet envisage le traitement de données personnelles, notamment dans le cadre de la délivrance d'agréments, de la création d'un registre national contenant des données à caractère personnel, ou encore de la vérification de l'honorabilité des membres de l'équipage.

4. Le présent avis se concentrera sur les questions liées à la protection des données qui sont soulevées par le projet de loi.

I. Sur l'agrément délivré par le ministre ayant la Santé dans ses attributions

5. L'article 3 du projet de loi a pour objectif de préciser que quiconque souhaitant exercer l'activité de transport sanitaire terrestre, que ce soit à titre principal ou accessoire, doit obligatoirement détenir un agrément délivré par le ministre ayant la Santé dans ses attributions (ci-après le « ministre »). L'article 4 soumet la délivrance de l'agrément à deux conditions cumulatives, à savoir, d'une

ANNEXES

part, celle de disposer d'une autorisation d'établissement et, d'autre part, celle de disposer des installations matérielles et techniques prévues à l'article 12 du projet de loi.

6. L'article 5 du projet de loi sous avis énumère les informations devant figurer dans la demande d'agrément adressée au ministre, parmi lesquelles se trouvent des données à caractère personnel. Ainsi, il ressort du paragraphe premier, point 1, de l'article précité que la demande d'agrément doit indiquer *« [...] les noms, prénoms, profession et domicile du demandeur, ou s'il s'agit d'une personne morale, la dénomination ou la raison sociale, la forme de la personne morale et son siège social, ainsi que les noms, prénoms, profession et domicile des directeurs, gérants ou administrateurs. »*

Selon le point 2, la demande d'agrément doit être accompagnée d'une attestation signée par la personne physique ou morale qui se propose d'exercer l'ac¬tivité de transport sanitaire terrestre, sans que l'objet de cette attestation soit toutefois défini.

En outre, le projet de loi sous avis prévoit dans le même paragraphe, au point 3, que les demandes d'agrément en question doivent *« comporter le(s) bulletin(s) n° 3 et 5 récents du casier judiciaire datant tous les deux de moins de trois mois à partir de la date d'introduction de la demande d'agrément tant du requérant que pour les directeurs, gérants et administrateurs visés au point 1°. »*

7. À l'instar de la Chambre des Métiers[17], la CNPD se demande dans quelle mesure les données personnelles énumérées à l'article 5 du projet de loi seraient pertinentes afin d'évaluer le respect des conditions d'obtention de l'agrément, énoncées à l'article 4 du même projet. Plus précisément, la Commission nationale s'interroge sur la pertinence d'inclure, par exemple, la profession et le domicile du directeur, du gérant ou de l'administrateur de l'entreprise ainsi que d'examiner les bulletins n°3 et 5 du casier judiciaire du demandeur d'agrément afin de vérifier si ce dernier est en possession *« d'une autorisation d'établissement ou du moins d'une décision de principe au sens de l'article 12, paragraphe 2, de la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales pour le métier secondaire de loueur d'ambulances »* et s'il dispose des *« installations matérielles et techniques prévues à l'article 12 »*.[18]

8. Tel que relevé dans l'avis de la Chambre des Métiers[19], l'honorabilité des dirigeants est appréciée lors de l'octroi de l'autorisation d'établissement. La Commission nationale estime également que les données personnelles requises et plus spécifiquement celles liées à la personne du directeur, gérant ou administrateur dans le cadre de la demande d'agrément, ne semblent pas être en conformité avec le principe de minimisation des données énoncé à l'article 5.1.c) du RGPD selon lequel les données à caractère personnel doivent être adéquates,

[17] Cf. avis de la Chambre des Métiers du 26 mai 2023, doc.parl. n°818/01 (ci-après l'« avis de la Chambre des Métiers »), points 1.1.2 et 2.2.
[18] Cf. article 4 du projet de loi.
[19] Cf. avis de la Chambre des Métiers, point 2.2.a).

pertinente et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

II. <u>Sur l'établissement d'un registre contenant des données à caractère personnel et de la transmission dudit registre au ministre compétent</u>

9. La loi en projet prévoit dans son article 10 *« qu'il est établi sous l'autorité du ministre un registre qui contient des données à caractère personnel et qui a pour finalités la gestion et le suivi administratif, le contrôle des demandes d'agrément, ainsi que la gestion des dossiers d'agréments et des agréments accordés »*. La Commission nationale se félicite que le texte sous avis détermine les finalités du registre, conformément au principe de limitations des finalités consacré à l'article 5.1.b) du RGPD, ainsi que le responsable du traitement, à savoir le ministre.[20]

10. Le deuxième paragraphe de l'article 10 du projet de loi mentionne que le registre porte sur les données énumérées à l'article 5. La CNPD renvoie à ses observations sous les points 7 et 8 du présent avis et attire l'attention des auteurs du projet de loi sur l'importance du principe de minimisation des données en vertu duquel seules peuvent être traitées les données nécessaires au regard des finalités énumérées à l'article 10.1 du projet de loi.

11. La CNPD se pose également la question de savoir si les informations concernant le certificat d'immatriculation, le certificat de contrôle technique du véhicule sanitaire, ainsi que l'attestation de police d'assurance certifiant la couverture de la responsabilité civile liée au véhicule sanitaire, dont la transmission par la SNCA au ministre est prévue à l'article 11.4 du projet de loi, font également l'objet d'un enregistrement dans le registre en question. En effet, le texte du projet de loi devrait énumérer de manière exhaustive les catégories de données susceptibles d'y figurer, tout en veillant à respecter le principe de minimisation des données.

12. Le paragraphe 4 de l'article 10 du projet de loi dispose que *« [s]eules les personnes qui en ont besoin dans l'exercice de leur fonction et de leurs tâches profes¬sionnelles ont accès au registre »*, ce qui est conforme au principe de sécurité et de confidentialité consacré aux articles 5.1.f) et 32 du RGPD. La CNPD regrette toutefois que le texte sous avis ne prévoit pas un système de journalisation des accès qui permettrait de contrôler le respect de ce principe. Sur ce point, la Commission nationale 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 pro¬cédure de contrôle.

13. Par ailleurs, il ressort du paragraphe 5 de l'article 10 que *« les données traitées sont irrémédiablement anonymisées ou détruites au plus tard à l'issue d'une durée de cinq ans après la fin de l'agrément ou, dans l'hypothèse que la demande d'agrément a été refusée, après la décision de refus. »* La

[20] Cf. article 10.3 du projet de loi.

ANNEXES

Commission nationale note favorablement que le projet de loi détermine la durée de conservation des données appelées à figurer dans le registre. Néanmoins, faute d'explications dans le commentaire de l'article quant à la nécessité de conserver les données pendant une durée de cinq ans après la fin de l'agrément ou la décision de refus, elle n'est pas en mesure d'apprécier si le principe de limitation de la conservation[21] est en l'espèce respecté.

14. L'article 10.6 du projet de loi indique que *« [l']accès des données à des tiers ne peut avoir lieu que sous une forme anonymisée »*. Concernant ce libellé, la CNPD suppose que les auteurs ont plutôt voulu viser l'accès des tiers aux données et non pas l'accès des données aux tiers. Par ailleurs, elle tient à souligner que le cadre légal posé par le RGPD ne s'applique pas aux données anonymes, voire anonymisées. Le considérant (26) du RGPD énonce à cet égard qu'il 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. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche. »* Il y a toutefois lieu de s'assurer qu'il s'agit effectivement de données anonymes et non pas de données pseudonymisées qui pourraient indirectement identifier une personne physique par le recours à des informations supplémentaires et qui, quant à elles, tombent dans le champ d'application du RGPD[22].

III. Sur la transmission de données par la SNCA au ministre

15. Aux termes de l'article 11.4 du projet, *« [e]n cas d'immatriculation d'un véhicule sanitaire, la SNCA fait parvenir sans délai, par voie électronique, au ministre les informations relatives au certificat d'immatriculation, au certificat de contrôle technique du véhicule sanitaire ainsi qu'à l'attestation de police d'assurance certifiant que la responsabilité civile à laquelle le véhicule sanitaire peut donner lieu est couverte. [...] »*.

16. Pour autant que des données se rapportant à des personnes physiques identifiées ou identifiables soient concernées, la disposition sous examen impose à la SNCA une obligation légale de transmettre des données personnelles au ministre, sans toutefois préciser les finalités pour lesquelles les données sont transmises. Ainsi, l'article 11.4 du projet de loi risque d'être contraire à l'article 6.3 du RGPD, lu ensemble avec l'article 6.1.c), en vertu duquel une disposition légale qui crée pour le responsable du traitement une obligation rendant nécessaire un traitement de données doit définir les finalités du traitement.

[21] Cf. art. 5.1.e) du RGPD

[22] A toutes fins utiles, la CNPD se permet de renvoyer à l'avis 05/2014 du groupe de travail « Article 29 » sur les techniques d'anonymisation, disponible sous : https://cnpd.public.lu/content/dam/cnpd/fr/publications/groupe-art29/wp216_en.pdf

17. Face au silence du texte sous avis, la Commission nationale n'est pas en mesure d'apprécier si le principe de proportionnalité, tel que garanti notamment par l'article 37 de la Constitution, ou encore le principe de minimisation des données est respecté.

IV. Sur le contrôle d'honorabilité des membres de l'équipage d'un véhicule sanitaire

18. Il découle de l'article 13 du projet de loi que chaque membre de l'équipage d'un véhicule sanitaire doit remplir différentes conditions, dont notamment le respect des exigences d'honorabilité telles que prévues par l'article 17 du projet de loi sous avis. Il ressort du premier paragraphe de l'article 17 précité que l'honorabilité s'apprécie *« sur base des antécédents judiciaires qui résultent du casier judiciaire »* tandis que les paragraphes subséquents énumèrent les infractions à considérer aux fins d'évaluer l'honorabilité d'un membre de l'équipage d'un véhicule sanitaire.

19. Bien que la CNPD comprenne la nécessité de contrôler l'honorabilité des membres d'équipage, elle déplore toutefois le manque de précision du texte concernant la manière dont le contrôle d'honorabilité sera effectué. Il serait souhaitable d'obtenir des précisions quels documents spécifiques et numéros de bulletins du casier judiciaire seront pris en considération à cette fin. De plus, il est à noter que le paragraphe 2 de l'article 17 semble comporter une énumération seulement exemplative (« en particulier ») des circonstances dans lesquelles les exigences en matière d'honorabilité sont satisfaites, ce qui amplifie l'insécurité juridique quant aux documents pouvant être consultés dans le cadre du contrôle d'honorabilité.

20. Par ailleurs, le texte sous avis ne spécifie pas clairement quel acteur est chargé d'effectuer le contrôle d'honorabilité. Il est nécessaire de clarifier si le contrôle en question relève de la responsabilité de l'employeur dans le cadre du processus de recrutement ou si le ministre compétent est l'entité en charge de ce contrôle.

En conséquence, la CNPD regrette le manque de précision de la disposition en question et recommande vivement de clarifier, d'une part, quel acteur sera chargé d'effectuer le contrôle susmentionné et, d'autre part, sur base de quels documents l'honorabilité sera vérifiée.

V. Sur la tenue et la transmission d'une liste des membres du personnel

21. L'article 18 du projet de loi impose aux transporteurs sanitaires l'obligation de maintenir à jour une liste des membres du personnel composant les équipages des véhicules sanitaires, en spécifiant leur niveau de formation, et de transmettre cette liste au ministre compétent de manière annuelle.

22. En l'absence d'indication de la finalité poursuivie par ce traitement, la CNPD se trouve dans l'incapacité de se prononcer sur la nécessité de cette mesure qui constitue une limitation du droit à l'autodétermination informationnelle et à la protection des données consacré à l'article 31 de la Constitution. S'y ajoute que l'article 18 du projet de loi risque d'être contraire à l'article 6.3 du RGPD, lu en combinaison avec l'article 6.1.c). Il résulte de ces dispositions que le

ANNEXES

droit de l'Union européenne ou le droit national d'un État membre qui crée pour le responsable du traitement une obligation légale rendant nécessaire un traitement de données doit définir les finalités du traitement.

23. Il est également impératif de fournir des clarifications concernant les catégories de données devant figurer sur cette liste qui sera transmise au ministre. Il est en effet primordial de définir avec précision les informations à inclure sur cette liste, d'autant plus que le fait de ne pas tenir à jour la liste des membres du personnel est sanctionné pénalement en vertu de l'article 23. En application des articles 31 et 37 de la Constitution, les données à transmettre par les transporteurs sanitaires au ministre doivent être limitativement énoncées au niveau de la loi[23] et respecter le principe de proportionnalité.

Ainsi adopté à Belvaux
en date du 23 février 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[23] Cf. en ce sens : avis du Conseil d'État 60.868 du 22 décembre 2023, doc. parl. n°7932/05, p. 10.

6

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8331 portant modification de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique et relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du carnet de vaccination électronique

Délibération n°9/AV4/2024
du 23 février 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

Le Comité européen de la protection des données (ci-après le « CEPD ») précise par ailleurs que pour toute limitation aux droits des personnes concernées adoptée au niveau des États membres, l'autorité de contrôle en matière de protection des données doit être consultée avant l'adoption d'une telle mesure par le parlement national[24].

2. Par courrier en date du 20 octobre 2023, le Ministère de la Santé a invité la Commission nationale à se prononcer sur le projet de loi n°8331 portant modification de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique (ci-après le « projet de loi »). Par ailleurs, ledit Ministère a saisi la CNPD par courrier du 25 octobre 2023 afin d'aviser le projet de règlement grand-ducal précisant les modalités et conditions de mise en place du carnet de vaccination électronique[25] (ci-après le « projet de règlement grand-ducal »). Le projet de

[24] Comité européen de la protection des données, Lignes directrices 10/2020 concernant les limitations au titre de l'article 23 du RGPD, Version 2.1, adoptées le 13 octobre 2021, point 68 (ci-après les « lignes directrices du CEPD concernant les limitations au titre de l'article 23 du RGPD »).

[25] L'article 1er du projet de loi vise à remplacer l'intitulé de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique par l'intitulé suivant : *« Loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique et la mise en œuvre d'un carnet de vaccination électronique ».*

ANNEXES

règlement grand-ducal est pris en exécution du futur article 4bis de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique et la mise en œuvre d'un carnet de vaccination électronique (ci-après le « futur article 4bis de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies »), tel qu'inséré après l'article 4 de ladite loi par l'article 2 du projet de loi susmentionné.

3. Bien que la Commission nationale ne souhaite nullement remettre en cause l'utilité de la mise en place d'un carnet de vaccination sous forme électronique (ci-après le « carnet digital ») visant à remplacer le carnet physique, dit « carte jaune », et ceci *« tant pour le bénéfice du patient que pour l'amélioration de l'efficacité et de la transparence des campagnes nationales de vaccination »*[26], 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.

4. De manière générale, la CNPD se félicite dans ce contexte que le projet de loi et le projet de règlement grand-ducal entendent conférer une base légale aux traitements de données effectués dans le cadre de la mise en place du carnet digital et de son utilisation subséquente. Elle note que le carnet digital vise, entre autres, à améliorer la prise en charge du patient en permettant au prestataire de soins de fournir des soins de santé de qualité, d'une part, et au patient de prendre une décision éclairée en matière de vaccination, d'autre part, tout en octroyant la possibilité à l'État de gérer les stocks des vaccins et suivre et évaluer la couverture vaccinale des vaccins recommandés.[27] Sa mise en place pourrait dès lors correspondre à une mission d'intérêt public conformément à l'article 6.1.e) du RGPD.

L'article 6.3 du RGPD prévoit dans ce contexte une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect 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. Dans ce cas de figure, le fondement et notamment les finalités des traitements de données doivent être spécifiquement prévus soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis et ce fondement doit répondre *« à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi. »*

5. Par ailleurs, dans la mesure où une partie des données traitées à travers le carnet digital sont relatives à la santé des patients en cause, celles-ci 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 spécifique 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.

[26] Voir exposé des motifs du projet de loi.
[27] Voir exposé des motifs du projet de loi, ainsi que les finalités mentionnées au futur article 4*bis* de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies, ainsi que le commentaire des articles, ad article 2.

La Commission nationale estime que les traitements de données mis en œuvre au moyen d'un carnet digital pourraient relever des motifs d'intérêt public dans le domaine de la santé publique visés à l'article 9.2.i) du RGPD, à condition que le droit de l'Union européenne ou le droit national prévoie des « mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée ».

6. En l'espèce, il convient de féliciter les auteurs du projet de loi et du projet de règlement grand-ducal d'avoir inséré dans les textes respectifs des précisons en matière de protection des données. Néanmoins, la CNPD tient à formuler des remarques sur certains points spécifiques.

I. <u>Quant au responsable du traitement</u>

7. La CNPD tient à rappeler que conformément à l'article 4.7) du RGPD, le responsable du traitement est *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; 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. »*

8. En ce qui concerne plus précisément les notions de responsable du traitement et de sous-traitant, il ressort des lignes directrices du CEPD sur ce sujet que *« [l]orsque le responsable du traitement est spécifiquement identifié par la loi, cette désignation est déterminante pour définir qui agit en tant que responsable du traitement. Cela présuppose que le législateur a désigné comme responsable du traitement l'entité qui est véritablement en mesure d'exercer le contrôle. »*[28]

9. Il est encore à noter que la notion de responsable du traitement, voire de responsabilité conjointe, sont des notions fonctionnelles en ce qu'elles visent à répartir les responsabilités en fonction des rôles réels joués par les parties. Ainsi, elles reposent sur une analyse factuelle plutôt que formelle.[29]

10. En l'espèce, le futur article *4bis* de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies prévoit que *« […] l'Agence nationale des informations partagées dans le domaine de la santé tient à la disposition des patients, des prestataires de soins et de l'autorité sanitaire un carnet de vaccination électronique ».* Dans le commentaire de l'article 2 du projet de loi, les auteurs expliquent, après avoir justifié la mise en place du carnet digital, que sa mise à disposition sera confiée à l'Agence nationale des informations partagées dans le domaine de la santé (ci-après l' « Agence eSanté »), car *« cette dernière assur[e] déjà la gestion de la plateforme électronique nationale avec le dossier de soins partagé. Cela permettra au carnet de vaccination électronique de bénéficier, par exemple, d'un niveau de*

[28] CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.0, adoptées le 7 juillet 2021, point 23.
[29] Page 3 et points 21 et 52 desdites lignes directrices.

ANNEXES

sécurité élevé tel que déjà assuré dans le cadre du dossier de soins partagé. »

11. Le texte du projet de loi engendre dès lors l'impression que l'Agence eSanté, créée sur base de l'article 60ter du Code de la sécurité sociale et soumise à l'autorité conjointe des ministres ayant dans leurs attributions la Santé et la Sécurité sociale, agirait seule en tant que responsable du traitement des données à caractère personnel opéré dans le cadre de la mise en œuvre du carnet digital. Néanmoins, la CNPD constate que des précisions se trouvent à cet égard dans le projet de règlement grand-ducal, ainsi que dans son commentaire des articles[30]. D'après sa lecture, il en ressort la configuration suivante :

- L'Agence eSanté sera responsable des traitements des données opérés par la création même du carnet digital pour chaque personne physique disposant d'un numéro d'identification national[31] et ceci à partir du premier encodage par le prestataire de soins. Par ailleurs, en vertu de l'article 1er (4) du projet de règlement grand-ducal, l'Agence eSanté doit procéder, dès réception d'un certificat de décès ou de la date de décès par le Centre des technologies de l'information de l'État, à l'archivage des données du carnet digital pendant la durée légale de conservation.

- Pour le traitement des données enregistrées par les prestataires de soins dans le carnet digital,[32] l'article 2 (1) du projet de règlement grand-ducal prévoit que lesdits prestataires agissent comme responsables conjoints avec l'Agence eSanté au sens de l'article 26 du RGPD.

- Finalement, pour le traitement des données enregistrées par l'autorité sanitaire[33] sur la gestion des stocks de vaccins et qui peuvent inclure des données à caractère personnel des prestataires de soins,[34] l'article 2 (2) du projet de règlement grand-ducal prévoit que l'autorité sanitaire agit avec l'Agence eSanté comme responsables conjoints au sens de l'article 26 précité du RGPD.

12. La CNPD a néanmoins des difficultés à relier les traitements précités opérés par les différents acteurs aux finalités mentionnées au futur article 4*bis* (2) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies. En d'autres termes, elle est d'avis qu'il ne ressort pas clairement des

[30] Voir par exemple le commentaire des articles, ad article 2 : « *Comme le carnet de vaccination électronique est créé sur la plateforme électronique nationale des informations partagées dans le domaine de la santé et que les prestataires de soins enregistrent les données en lien avec les vaccinations de leurs patients comme ils le font actuellement sur la carte jaune papier, le présent projet de règlement grand-ducal entérine ce partage des responsabilités en instituant une responsabilité conjointe entre ces deux intervenants. Il en va de même pour les données concernant la gestion des stocks de vaccins enregistrées par l'autorité sanitaire et qui peuvent inclure les données à caractère personnel des prestataires de soins à qui sont distribués des vaccins.* »

[31] Le commentaire de l'article 1er du projet de règlement grand-ducal précise qu' « *[à] terme, un carnet de vaccination électronique devrait par conséquent être créé pour toute personne résidente et toute personne non-résidente affiliée à la Caisse nationale de santé.* »

[32] Le futur article 4bis (4) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies prévoit en effet que ce sont les prestataires de soins qui « *enregistrent au moment de la vaccination et au plus tard endéans le soixante-douze heures de celle-ci dans le carnet de vaccination électronique les données visées au paragraphe (3) pour toute vaccination recommandée par l'État. […]*»

[33] D'après l'article 2 de l'actuelle loi du 1er août 2018 sur la déclaration obligatoire de certaines maladies, le directeur de la santé ou son délégué sont à désigner comme « autorité sanitaire ».

[34] Voir commentaire des articles du projet de règlement grand-ducal, ad article 2.

textes sous avis pour quelles des différentes finalités poursuivies l'Agence eSanté, l'autorité sanitaire, ainsi que les prestataires de soins de santé sont à considérer comme responsable, voire comme responsables conjoints des traitements mis en œuvre à travers le carnet digital.

13. Dès lors, en prenant en compte que la protection des données à caractère personnel est une matière réservée à la loi par la Constitution, d'une part, et que dans de telles matières l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc,[35] la Commission nationale recommande aux auteurs du projet de loi de préciser dans le corps du texte qui est à qualifier de responsable, voire de responsable(s) conjoint(s) des traitements en distinguant entre les différentes finalités à atteindre.

14. Finalement, il convient de mentionner que l'article 26.1 du RGPD dispose que les responsables conjoints du traitement 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. Les lignes directrices du CEPD à ce sujet prévoient qu'il *« convient de répartir les responsabilités en matière de conformité, ainsi qu'il résulte de l'utilisation du terme « respectives » à l'article 26, paragraphe 1. Cela n'exclut pas que le droit de l'Union ou le droit d'un État membre puisse déjà établir certaines responsabilités de chaque responsable conjoint du traitement. Si tel est le cas, l'accord entre les responsables conjoints du traitement devrait également couvrir toute responsabilité supplémentaire nécessaire aux fins d'assurer le respect des exigences du RGPD qui ne sont pas couvertes par les dispositions légales. »*[36]

15. Les paragraphes (3) et (4) de l'article 2 du projet de règlement grand-ducal précisent dans ce contexte les modalités d'exercice des droits des personnes concernées. La CNPD tient dès lors à rendre attentifs les auteurs du projet de règlement grand-ducal qu' *« [i]l ne s'agit que de définir, dans leurs relations internes, quelle partie est tenue de répondre aux demandes des personnes concernées. »*[37] En effet, indépendamment des termes de l'accord entre responsables conjoints, la personne concernée peut contacter chacun des responsables conjoints du traitement conformément à l'article 26.3 du RGPD.

II. <u>Quant aux données à caractère personnel collectées</u>

16. Au titre du respect des principes relatifs au traitement des données à caractère personnel tels qu'ils sont prévus par le

[35] Voir articles 31 et 37 de la Constitution luxembourgeoise. D'après la jurisprudence de la Cour constitutionnelle, l'article 45, paragraphe 2, de la Constitution exige en effet que dans ces matières, *« la fixation des objectifs des mesures d'exécution doit être clairement énoncée, de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi »* (Cour constitutionnelle, 4 juin 2021, n° 166, Mém. A n° 440 du 10 juin 2021 et Cour constitutionnelle, 3 mars 2023, n° 177, Mém. A, n° 127 du 10 mars 2023).

[36] Point 162 desdites lignes directrices.

[37] Point 165 desdites lignes directrices.

ANNEXES

RGPD, la CNPD rappelle que les données à caractère personnel doivent être *« collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités [...] (limitation des finalités) » et qu'elles doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données). »*[38]

17. La CNPD estime que le futur article 4*bis* (2) et (3) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies respecte les exigences susmentionnées. À des fins de sécurité juridique, elle conseille uniquement aux auteurs du projet de loi de préciser plus en détail dans le corps du texte quelles données ou catégories de données sont visées par les termes *« données administratives du patient »* et *« donnes administratives du prestataire de soins vaccinateur »* prévus aux points 1° et 4° dudit paragraphe (3).

18. Néanmoins, la CNPD a des difficultés à saisir le déroulement concret de la création du carnet digital et elle se pose des questions pratiques sur le traitement initial des données à caractère personnel y incluses. En effet, il ressort d'une lecture combinée du futur article 4*bis* (4) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies et de l'article 1 (1) du projet de règlement grand-ducal que les prestataires de soins doivent enregistrer au moment de la vaccination ou au plus tard soixante-douze heures après les données des patients dans le carnet digital, alors que la création même du carnet digital par l'Agence eSanté n'intervient qu'à partir du premier encodage par le prestataire de soins. Le commentaire de l'article 1er du projet de règlement grand-ducal précise dans ce contexte qu'afin que l'Agence eSanté ne crée pas *« [...] indistinctement un carnet de vaccination électronique pour toute personne disposant d'un numéro d'identification national mais non d'une vaccination, il est indiqué au vu des principes de minimisation du traitement des données à caractère personnel et d'efficacité administrative de ne créer un carnet de vaccination électronique qu'à partir du premier encodage. »*

Or, comment un prestataire de soins peut déjà encoder lors d'une vaccination les données listées au futur article 4bis (3) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le carnet digital si l'Agence ne le crée qu'à partir du premier encodage par ce même prestataire ? Soit le carnet digital a déjà été créé par l'Agence eSanté et existe dès lors au moment du premier encodage par le prestataire de soins, soit ce dernier doit demander la création d'un carnet digital à l'Agence eSanté lors d'une vaccination et ce n'est que postérieurement qu'il peut y encoder lesdites données. La CNPD estime dès lors primordial que des clarifications à ce sujet soient intégrées dans les deux projets de textes légaux.

19. Par ailleurs, la CNPD note que le futur article 4*bis* (5) de la loi modifiée du

[38] Voir article 5.1.b) et e) du RGPD.

1er août 2018 sur la déclaration obligatoire de certaines maladies prévoit que les données des personnes vaccinées contre la COVID-19[39] sont transférées au carnet digital. Elle comprend que ce transfert se justifie, notamment afin que les personnes continuent à bénéficier d'une preuve de vaccination en cas de dommages ou de demandes de suivi d'effets indésirables et leur permet de garder trace de leur vaccination contre la COVID-19.[40]

Dans ce contexte, la Commission nationale se demande si les personnes concernées ont aussi la possibilité de demander que des informations sur d'éventuelles anciennes vaccinations contenues sur leur carte jaune sont de même transférées vers le carnet digital.

20. Finalement, comme le futur article 4*bis* (4) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies prévoit que le patient doit consentir à l'enregistrement des données relatives aux futures vaccinations autres que celles recommandées par l'État, la CNPD tient à insister que toutes les conditions d'un consentement valide au sens du RGPD sont à respecter, notamment que le consentement doit être libre, spécifique, éclairé et univoque.[41]

III. Quant à l'accès aux données à caractère personnel

21. D'après l'article 3.1 du projet de règlement grand-ducal, le carnet digital est accessible par le patient, le prestataire de soins, ainsi que l'autorité sanitaire via la plateforme électronique d'échange et de partage de données de santé visée à l'article 60*ter* du Code de la sécurité sociale. De même, il y est indiqué que le prestataire de soins peut *« également accéder au carnet de vaccination depuis un programme informatique conforme aux dispositions de l'article 11, paragraphe (2) et de l'article 12, à l'exception de son paragraphe (2), alinéa 4, point (b), du règlement grand-ducal modifié du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé. »* D'après le commentaire de l'article 3 du projet de règlement grand-ducal, l'Agence eSanté doit s'assurer dans un tel cas de figure que la connexion envisagée garantit un niveau de sécurité approprié et que la procédure sur l'interopérabilité du programme informatique visée à l'article 12 du règlement grand-ducal du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé est à appliquer.

La CNPD rend attentif les auteurs du projet de règlement grand-ducal au fait que le règlement grand-ducal précité du 6 décembre 2019 prévoit les modalités de sécurité et d'interopérabilité dans ses articles 10 et 11 et non dans ses articles 11 et 12 comme mentionné actuellement par l'article 3.1 du projet de règlement grand-ducal.

22. En ce qui concerne l'accès aux données contenues dans le carnet digital et sous

[39] Traitées sur base de l'article 10 (2), point 3°, point b) de la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19.
[40] Voir commentaire des articles du projet de loi, ad article 2.
[41] Voir définition du consentement à l'article 4 point 11 du RGPD, ainsi que les conditions applicables au consentement prévues à l'article 7 du RGPD.

ANNEXES

réserve de ses commentaires au point 12 du présent avis, la CNPD constate que le futur article 4*bis* (6), deuxième alinéa de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies prévoit que l'autorité sanitaire peut accéder à des données pseudonymisées pour toutes les huit finalités énoncées au paragraphe (2) dudit article, tandis qu'un accès aux données nominatives n'est limitativement prévu que pour trois des huit finalités.

La CNPD se permet dès lors de rappeler qu'en pratique, la pseudonymisation consiste à remplacer les données directement identifiantes (telle que le nom, prénom ou l'adresse exacte) d'un jeu de données par des données indirectement identifiantes comme par exemple un alias ou un numéro séquentiel. La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. Contrairement à l'anonymisation, la pseudonymisation est une opération réversible. Il est dès lors possible d'identifier indirectement une personne si l'on dispose d'informations supplémentaires.

Le considérant (26) du RGPD précise dans ce contexte que les *« données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. »*

23. La CNPD se pose dès lors la question qui sera en charge de la pseudonymisation des données, et préalablement à quelle action. Alors que les données ne peuvent en principe être pseudonymisées qu'après leur enregistrement dans le carnet digital, il ne ressort pas des textes sous avis à qui incomberait la tâche de la pseudonymisation. Elle pourrait être effectuée par un « tiers de confiance », qui doit être compris comme une personne physique ou morale habilitée à effectuer des opérations de sécurité juridique dont des services de pseudonymisation ou d'anonymisation et qui présente des garanties d'indépendance, de compétence et ne se trouvant pas en situation de conflit d'intérêts au regard des données qu'il traite dans le cadre de ses diverses activités.

24. Elle se demande de même comment en pratique il sera garanti que l'autorité sanitaire aura accès à des données nominatives pour certaines finalités, tandis qu'elle pourra uniquement accéder à des données pseudonymisées pour d'autres finalités et qui devra s'assurer que cette limitation soit respectée.

6

25. La CNPD constate avec satisfaction que l'article 4.1 du projet de règlement grand-ducal prévoit un système de journalisation des accès, c'est-à-dire un enregistrement des données d'identification de la personne qui a consulté ou enregistré une ou plusieurs données au carnet digital, ainsi que le contexte de son intervention. Selon ledit article, les *« données de journalisation suivent le même cycle de vie que les données auxquelles elles se rapportent »*, c'est-à-dire que la durée de conservation des logs est la même que celle des données du carnet digital.[42] Comme le futur article 4*bis* (8) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies prévoit que les données contenues dans le carnet digital sont sauvegardées pendant trente ans suite à leur encodage par le prestataire de soins, il en ressort que les données de journalisation seraient conservées aussi pendant trente ans.

26. Néanmoins, alors que les fichiers de journalisation peuvent être considérés comme un élément servant à remplir l'obligation de sécurité découlant de l'article 32 du RGPD en évitant des accès non-autorisés aux données à caractère personnel, les données de ces fichiers permettant d'identifier des personnes ne doivent, comme toutes les données à caractère personnel, pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées conformément à l'article 5.1.e) du RGPD.

27. Les fichiers de journalisation peuvent aussi avoir comme finalité d'assurer le droit d'accès de la personne concernée à des données à caractère personnel la concernant, et plus particulièrement aux données relatives aux destinataires des données conformément à l'article 15.1.c) du RGPD. En particulier, ils peuvent avoir comme finalité de permettre de retracer qui a eu accès à des données à caractère personnel.

Pour ce type de fichiers de journalisation, un des critères à prendre en considération est en effet la durée de conservation des données auxquelles les données des fichiers de journalisation se rapportent, c'est-à-dire les données dont les communications à d'autres personnes sont retracées par les fichiers de journalisation en question.

Or, la Cour de justice de l'Union européenne a estimé que *« la durée de conservation des données de base peut constituer un paramètre utile sans toutefois être déterminant »*. Par ailleurs, elle a décidé qu' *« une réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêts et obligations en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement ».*[43]

[42] Voir commentaire des articles du projet de règlement grand-ducal, ad article 4.
[43] CJUE, arrêt du 7 mai 2009, C-553/07, EU:C:2009:293, points 58 et 66.

ANNEXES

28. Sur base de ce qui précède, la CNPD se permet de rappeler sa recommandation de conserver les fichiers de journalisation pendant une période de cinq ans, alors que ce délai correspond également au délai de prescription en matière délictuelle (comme par exemple la violation du secret professionnel sanctionnée par l'article 458 du Code pénal), sauf lorsqu'une procédure de contrôle est en cours.

29. Finalement, elle constate que le commentaire des articles du projet de loi prévoit ce qui suit : « Concernant les données pseudonymisées et notamment dans le cadre du suivi et de l'évaluation de la couverture vaccinale de l'effectivité des vaccins recommandés par l'État, l'accès devrait permettre un croisement avec d'autres sources de données, par exemple socio-démographique, afin d'obtenir les résultats les plus pertinents permettant de prendre les mesures qui s'imposeraient en vue de protéger les populations les plus vulnérables. » Sans précisions supplémentaires, la Commission nationale se demande dès lors quelles sont ces « autres sources de données », d'une part, et si des croisements avec des données à caractère personnel contenues dans d'autres fichiers étatiques sont prévues, d'autre part.

IV. <u>Quant au droit d'opposition</u>

30. Il ressort du futur article 4*bis* (7) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies que ni les patients, ni les prestataires de soins ne peuvent s'opposer à l'enregistrement de leurs données dans le carnet digital, d'une part, et qu'ils sont informés de cette limitation avant le premier enregistrement de leurs données, d'autre part. L'article 1er (2) du projet de règlement grand-ducal énonce dans ce contexte qu'il revient au prestataire de soins de fournir au patient, avant la création de son carnet digital, *« l'information relative au traitement des données à caractère personnel et notamment à la limitation du droit d'opposition ».*

Le commentaire de l'article 2 du projet de loi quant à lui contient des justifications sur la nécessité de limiter le droit d'opposition des personnes concernées *« afin de pouvoir réaliser les finalités de santé publique pour lesquelles le carnet de vaccination électronique est mis en place et en particulier en vue de déterminer le taux de couverture vaccinale ainsi que pour assurer la traçabilité et gérer les stocks de vaccins distribués par l'État ».* Il y est précisé aussi que c'est *« dans l'intérêt de la santé publique de limiter le droit individuel des personnes à s'opposer à l'enregistrement de leurs données à caractère personnel »* et qu'une telle *« mesure s'avère nécessaire et proportionné car sans cette dernière le bénéfice du carnet [digital] ne pourra être réalisé ».*

31. La CNPD tient tout d'abord à souligner que par principe, toute personne concernée dispose du droit de s'opposer *« à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions »* conformément à l'article 21 du RGPD. Dans ce cas, *« le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent*

sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. »[44]

32. Des limitations à la portée dudit droit peuvent être prévues par le droit de l'Union européenne ou le droit d'un État membre par voie de mesure législative sur base de l'article 23 du RGPD. Or, ledit article prévoit en son paragraphe 1er que les droits de la personne concernée peuvent être limités lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs énumérés dans ce paragraphe.

Par ailleurs, il y a lieu de soulever que lorsqu'une telle restriction aux droits des personnes est prévue par une mesure législative, elle doit contenir des dispositions spécifiques relatives aux informations énumérées au paragraphe 2 de l'article 23 du RGPD.[45]

33. Il y a donc lieu de vérifier la conformité de la limitation du droit d'opposition prévue par le futur article 4*bis* (7) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies avec les exigences précitées de l'article 23 du RGPD.

34. Le CEPD a clarifié que la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme exigent que « *les mesures législatives qui visent à limiter l'étendue des droits des personnes concernées ou des obligations du responsable du traitement soient prévisibles pour les personnes concernées.*»[46] De même, l'analyse et le constat de nécessité et de proportionnalité d'une limitation sur base d'une mesure législative devraient être effectués par le législateur avant qu'il décide de prévoir une restriction.[47]

Par ailleurs, *« [l]e lien entre les limitations prévues et l'objectif poursuivi devrait être clairement indiqué dans la mesure législative.»*[48]. Ce lien doit donc y être expressément précisé.

35. La CNPD note que d'après les auteurs du projet de loi et leur commentaire des articles, la mesure de limitation du droit d'opposition des personnes concernées constitue une mesure nécessaire et proportionnée afin de garantir la réalisation des finalités de santé publique pour lesquelles le carnet digital est mis en place, en particulier la détermination du taux de couverture vaccinale, ainsi que la traçabilité et la gestion des stocks de vaccins distribués par l'État. Elle comprend dès lors que ladite limitation pourrait viser à garantir un objectif important d'intérêt

[44] Voir article 21.1, deuxième phrase du RGPD.
[45] Il s'agit des finalités du traitement ; des catégories de données à caractère personnel; de l'étendue des limitations introduites ; des garanties destinées à prévenir les abus ou l'accès ou le transfert illicites; la détermination du responsable du traitement; les durées de conservation et les garanties applicables ; les risques pour les droits et libertés des personnes concernées et le droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation.
[46] Lignes directrices du CEPD concernant les limitations au titre de l'article 23 du RGPD, point 17.
[47] Lignes directrices du CEPD concernant les limitations au titre de l'article 23 du RGPD, point 40.
[48] Lignes directrices du CEPD concernant les limitations au titre de l'article 23 du RGPD, point 21.

ANNEXES

public dans le domaine de la santé publique conformément à l'article 23.1.e) du RGPD.

Or, la Commission nationale constate que les explications à ce sujet dans le commentaire des articles du projet de loi ne sont pas suffisantes, car elles ne se trouvent pas dans le projet de loi lui-même et ne permettront pas à la personne concernée de comprendre le lien entre la limitation du droit d'opposition et la sauvegarde des intérêts publics dans le domaine de la santé publique une fois le texte adopté. En particulier, il y a lieu de préciser dans le texte du projet de loi comment la limitation du droit d'opposition contribuerait à garantir la santé publique. Conformément au considérant 8 du RGPD, la raison de la limitation devrait en effet être compréhensible pour les personnes auxquelles cette limitation s'applique.

36. En ce qui concerne les finalités du traitement[49], il s'agit de préciser pourquoi le droit d'opposition de la personne concernée est limité (et pas les finalités du traitement opéré en général). La disposition sous revue doit être compréhensible pour les personnes auxquelles elle s'applique, ce qui implique une compréhension claire de comment et quand la limitation s'applique.

De même, l'article 23.2.g) du RGPD exige que la mesure législative tienne compte des risques que les limitations font peser sur les droits et libertés de la personne concernée. Il s'agit d'une précision textuelle législative très importante, qui contribue à l'évaluation de la nécessité et de la proportionnalité des limitations.

Des précisions sur ces deux points devraient dès lors être intégrées dans le corps du texte du projet de loi.

37. Finalement, le CEPD est d'avis qu'*« une exclusion générale des droits des personnes concernées à l'égard de l'ensemble ou de certaines opérations de traitement de données ou à l'égard de certains responsables du traitement ne respecterait pas l'essence du droit fondamental à la protection des données à caractère personnel tel qu'il est consacré par la Charte ».*[50]

L'homologue français de la CNPD, la Commission nationale de l'informatique et des libertés (CNIL), a également estimé que *« [l]es limitations prévues par le droit doivent donc être proportionnées et ne pas aboutir à remettre en cause de façon générale les droits garantis par le RGPD. À cet égard, devraient ainsi être proscrites :*

- *l'exclusion, pour un même traitement, de l'ensemble des droits prévus par le RGPD*
- *tout comme l'exclusion générale du droit d'opposition pour tous les traitements mis en œuvre par une collectivité publique. »*[51]

38. La Commission nationale ne peut que se rallier à ces constats. Dès lors, il est

[49] Prévu par l'article 23.2. point a) du RGPD.
[50] Lignes directrices du CEPD concernant les limitations au titre de l'article 23 du RGPD, point 14.
[51] Article de la CNIL *« Droit d'opposition : les conditions de dérogation en vertu de l'article 23 du RGPD »* du 1er juin 2023, disponible sous : « https://www.cnil.fr/fr/droit-dopposition-les-conditions-de-derogation-en-vertu-de-larticle-23-du-rgpd.

primordial que tous les autres droits conférés aux personnes concernées par les articles 12 à 20 et 22 du RGPD soient pleinement respectés par les différents responsables du traitement en cause, c'est-à-dire par l'Agence eSanté, l'autorité sanitaire, ainsi que les différents prestataires de soins de santé. Par ailleurs, la limitation du droit d'opposition ne peut uniquement viser les traitements de données à caractère personnel mis en œuvre à travers le carnet digital et en aucun cas d'autres traitements opérés par lesdits responsables du traitement.

Ainsi adopté à Belvaux
en date du 23 février 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8250 concernant le comptage divisionnaire et la répartition des coûts de chaleur, de froid et d'eau chaude sanitaire et au projet de règlement grand-ducal concernant le comptage divisionnaire et la répartition des coûts de chaleur, froid et eau chaude sanitaire et modifiant le 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

Délibération n°10/AV5/2024
du 23 février 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Par courrier en date du 11 septembre 2023, Monsieur le Ministre de l'Énergie et de l'Aménagement du territoire a invité la Commission nationale à se prononcer au sujet du projet de loi n°8250 concernant le comptage divisionnaire et la répartition des coûts de chaleur, de froid et d'eau chaude sanitaire (ci-après le « projet de loi ») qui avait déjà été déposé le 14 juin 2023 à la Chambre des députés et pour lequel un traitement prioritaire avait été demandé au Conseil d'État. Il est à noter qu'en même temps, un projet de règlement grand-ducal[52] visant à mettre en œuvre certaines dispositions du projet de loi avait été déposé sans que la CNPD n'ait cependant été saisie pour avis. Elle s'autosaisit partant pour le projet de règlement grand-ducal afin de faire part de ses observations.

3. Le projet de loi entend transposer en droit national la directive (UE) 2018/2002 du Parlement européen et du Conseil du 11 décembre 2018 modifiant la directive 2012/27/UE relative à l'efficacité énergétique

[52] Projet de règlement grand-ducal concernant le comptage divisionnaire et la répartition des coûts de chaleur, froid et eau chaude sanitaire et modifiant le 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 (ci-après le « projet de règlement grand-ducal »).

qui établit un cadre commun de mesures pour la promotion de l'efficacité énergétique dans l'Union. Il ressort de l'exposé des motifs du projet de loi que la directive (UE) 2018/2002 impose *« aux États membres de créer un nouveau cadre légal qui rend obligatoire le comptage de la consommation de certains types d'énergie au niveau des unités individuelles d'un immeuble collectif ».* L'objectif poursuivi est d'inciter les utilisateurs finals, par la mise à disposition régulière des informations sur leur consommation d'énergie réelle, de réaliser des économies d'énergie par changement comportemental.

4. Le présent avis ne se prononcera pas sur les directives susmentionnées mais se limitera à examiner les dispositions du projet de loi ainsi que du projet de règlement grand-ducal qui concernent leur mise en œuvre concrète en droit national ayant un impact en matière de protection des données personnelles.

I. Observations générales

5. Il convient de rappeler que les informations collectées par les compteurs d'énergie thermique constituent des données à caractère personnel si elles peuvent être reliées à une personne physique identifiée ou identifiable. Déjà lors du déploiement national des compteurs intelligents, la Commission nationale avait, tout en reconnaissant les avantages apportés par ces compteurs, mis en garde contre les risques qui pourraient se poser pour la protection de la vie privée[53]. À titre d'exemple, l'analyse des données collectées permet de déduire un grand nombre d'informations sur les habitudes de vie des personnes concernées, telles que les heures de lever et de coucher, les périodes d'absence, le nombre de personnes présentes dans le logement ou même, dans des cas spécifiques, le type d'appareils utilisés.

6. Plus particulièrement, la CNPD avait rendu un avis sur ce qui allait devenir le règlement grand-ducal du 27 août 2014 relatif aux modalités du comptage de l'énergie électrique et du gaz naturel, texte pris en exécution des lois modifiées du 1er août 2007 relative à l'organisation du marché de l'électricité respectivement du gaz naturel[54]. En ce qui concerne les traitements effectués à partir des données collectées par les compteurs intelligents, la CNPD avait notamment souligné l'importance de déterminer le ou les responsables du traitement ainsi que les finalités pour lesquelles les données sont traitées, tout comme une durée de conservation proportionnée. Force est de constater que ces remarques restent valables pour le texte actuellement sous examen (Cf. points 10, 12 et 24 du présent avis).

7. La Commission nationale se demande par ailleurs comment le projet de loi s'articule avec les lois précitées du 1er août 2007 ainsi qu'avec les textes pris en leur exécution. Se pose également la question d'un risque de

[53] https://cnpd.public.lu/fr/actualites/national/2014/05/smart-metering-lux-metering.html.
[54] Délibération n°566/2013 du 13 décembre 2013 de la Commission nationale pour la protection des données, consultable sur https://cnpd.public.lu/fr/decisions-avis/2013/comptage-energie-gaz.html

ANNEXES

chevauchement et de contradiction entre la loi en projet et les différents textes existants.

II. <u>Sur l'installation des appareils de mesure</u>

8. Selon la compréhension de la CNPD, le projet de loi prévoit le déploiement de trois différents types d'appareils de mesure, à savoir :

- les compteurs visés au point 1° de l'article 2.1 qui sont installés par le gestionnaire de réseau au point de raccordement de chaque client final ;
- les compteurs individuels visés au point 2° de l'article 2.1 qui sont installés dans les immeubles collectifs par le propriétaire ou, dans le cas d'une copropriété, par le syndic au point de raccordement des unités privatives. Ces compteurs individuels sont installés si les occupants des unités privatives n'ont pas de lien contractuel direct avec le fournisseur d'énergie et ne sont, par conséquent, pas des clients finals ;
- les répartiteurs de frais de chauffage visés à l'article 5 qui sont installés dans les immeubles collectifs par le propriétaire ou, dans le cas d'une copropriété, par le syndic si l'installation de compteurs individuels n'est pas techniquement réalisable ou économiquement justifiée.

À la connaissance de la CNPD les contrats d'énergie et les compteurs liés sont en principe signés et affectés au nom du locataire ou de l'occupant final y compris en cas de copropriété. Nous ignorons si des cas de figure exceptionnels seraient à ce jour encore susceptibles d'exister sur le territoire du Grand-Duché de Luxembourg, en particulier depuis l'installation et le déploiement des compteurs intelligents et, par conséquent, que l'ensemble des cas de figure visés ci-avant sous la liste du point 8 du présent avis soient vraisemblablement susceptibles de refléter la réalité de la situation juridique nationale.

9. Si le projet de loi indique bien qui est responsable de l'installation des différents appareils de mesure, il reste cependant muet quant aux différents traitements de données qui seront effectués en application du texte. Ainsi, le projet de loi ne fournit ni d'indication sur la personne qui procède au relevé des différents appareils de mesure ni sur celle étant à considérer comme responsable des différents traitements qui en résultent.

10. En ce qui concerne l'installation des compteurs par les gestionnaires de réseau, il ressort de l'alinéa 3 de l'article 3.1 du projet de loi que ces gestionnaires doivent fournir aux clients finals des informations *« en ce qui concerne la collecte et le traitement des données à caractère personnel conformément à la législation en matière de protection des données et de la vie privée ».* La CNPD suppose que cette disposition fait référence à l'obligation de transparence incombant au responsable du traitement en vertu des articles 12 et suivants du RGPD de sorte qu'il est possible d'en déduire que les gestionnaires de réseau sont à considérer comme responsables du traitement. Pour des raisons de sécurité juridique, il serait toutefois préférable que le projet de loi détermine expressément qui est le responsable du traitement. En effet, la notion de responsable du traitement

joue un rôle important dans l'application du RGPD dans la mesure où elle détermine qui est responsable des différentes règles en matière de protection des données, telles que la sécurité du traitement, ainsi que la manière dont les personnes concernées peuvent exercer leurs droits[55]. En l'absence de clarté sur la désignation du responsable de traitement se pose notamment la question de l'attribution de la responsabilité de la mise en place des mesures techniques et organisationnelles telle que prévu par l'article 24 du RGPD.

11. Dans ce contexte, il est à noter que l'obligation de fournir des informations relatives au traitement des données personnelles, lors de l'installation des compteurs, n'est énoncée que pour les gestionnaires de réseau, et non pas pour les propriétaires ou les syndics dans le cas d'une copropriété, lors de l'installation de compteurs individuels et tels que mentionnés à l'article 3.2 du projet de loi. Cette façon de procéder soulève des interrogations, étant donné que les propriétaires et syndics pourraient alors être considérés comme responsables du traitement en ce qui concerne les données collectées par les compteurs individuels et les répartiteurs de chauffage si l'on s'en tient littéralement au texte du projet de loi et aux cas de figure tels qu'énoncés au deuxième et au troisième tirets du point 8 du présent avis. Comme exposé préalablement, la CNPD se demande si ces cas exceptionnels sont encore susceptibles de refléter la réalité de la situation juridique nationale actuelle. A supposer de telles exceptions existantes, la CNPD tient à rappeler que les propriétaires et les syndics auraient également une obligation de transparence vis-à-vis des personnes concernées en application des articles 12 et suivants du RGPD.

12. Le texte sous examen reste par ailleurs muet quant aux catégories de données collectées, les finalités poursuivies, la durée de conservation ou encore les destinataires auxquels les données peuvent être communiquées. Ce manque de précision est d'autant plus regrettable alors que les données collectées par les différents appareils de mesure sont susceptibles de fournir une vue très détaillée sur les habitudes personnelles de consommation des personnes concernées[56]. Plus particulièrement, en l'absence de détermination claire des finalités, il y a un risque accru que le propriétaire utilise les données collectées relatives à la consommation d'énergie des occupants – lorsque ces derniers ne seraient pas directement liés contractuellement avec le fournisseur d'énergie si tant est qu'une telle situation juridique exceptionnelle soit susceptible d'exister au Luxembourg – à des finalités qui ne sont pas compatibles avec l'objectif poursuivi par la directive que le projet de loi entend transposer. Pour rappel, celui-ci a trait à la répartition des coûts de l'énergie basée sur les consommations réelles et la mise à disposition régulière des informations sur la consommation

[55] V. en ce sens: Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 3., disponibles sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr

[56] Cf. point 5 du présent avis.

ANNEXES

d'énergie réelle pour que les occupants puissent réaliser des économies d'énergie par changement comportemental. Ainsi, le principe de limitation des finalités consacré à l'article 5.1.b) du RGPD s'oppose en principe à ce que le propriétaire puisse se baser sur ces données à d'autres fins que celles liées à la simple information en termes d'efficacité énergétique des occupants.

III. <u>Sur la mise à disposition des informations relatives à la consommation et à la facturation</u>

13. Aux termes de l'article 2.3 du projet de loi, *« [l]es fournisseurs ainsi que les propriétaires ou, en cas de copropriété, les syndics sont soumis à des obligations de mise à disposition des données et informations relatives à la facturation et la consommation conformément aux dispositions de l'article 11 ».* Pour ce qui est des compteurs installés par les gestionnaires de réseau, l'obligation de mise à disposition des données incombe au fournisseur et non pas au gestionnaire de réseau, ce qui semble supposer une transmission de données entre le gestionnaire de réseau et le fournisseur. Il est regrettable que le projet de loi n'indique pas clairement quelles données sont transmises et pour quelles finalités.

14. L'article 11 du projet de loi précise les obligations de mise à disposition d'informations visées à l'article 2.3. L'article 11.1 s'applique à la relation entre le fournisseur et le client final et ne soulève pas d'observations particulières de la part de la CNPD quant à la protection des données.

À titre indicatif, la CNPD tient seulement à mentionner que l'article 7.1.4° du projet de règlement grand-ducal prévoit en guise des informations minimales devant figurer dans la facture ou dans les documents fournis en même temps un simple renvoi à des coordonnées génériques et non ciblées d'associations de défense de clients finals, d'agences de l'énergie ou d'organismes en matière similaires. Or le point 9.3 de la recommandation (UE) 2019/1660 de la Commission européenne du 25 septembre 2019 relative à la mise en œuvre des nouvelles dispositions de la directive 2012/27/UE relative à l'efficacité énergétique en matière de mesure et de facturation[57] (ci-après la « recommandation (UE) 2019/1660 ») mentionne l'intérêt pour les États membres transposant la nouvelle annexe VII bis d'indiquer *« les éventuels services de médiation ou de règlement extrajudiciaire des litiges qui sont juridiquement compétents pour traiter les plaintes et les litiges relatifs au comptage, au comptage divisionnaire, à la facturation et à la répartition des coûts »* afin que les fournisseurs ou autres acteurs puissent aussi inclure ces données sur les factures.

15. Les paragraphes 2 et 3 de l'article 11 s'appliquent aux situations où les occupants ne sont pas des clients finals. À supposer, comme exposé préalablement, qu'une telle situation juridique soit encore existante sur le territoire national, ces dispositions prévoient que le propriétaire ou, en cas de copropriété, le syndic communique une note d'évaluation contenant des informations relatives à la facturation ou à la consommation établies

[57] Disponible sous : https://eur-lex.europa.eu/eli/reco/2019/1660

sur base de la consommation réelle ou des relevés des répartiteurs des frais de chauffage ainsi qu'une note d'information sur la consommation en chaleur, froid et eau chaude sanitaire aux occupants des unités privatives.

16. À cet égard, il est à noter que la directive indique qu'il appartient aux États membres de décider qui doit être chargé de fournir les informations aux utilisateurs finals sans contrat direct ou individuel avec un fournisseur d'énergie[58]. La recommandation (UE) 2019/1660 précise en son point 7.2 que *« les entités les mieux placées pour informer les utilisateurs finals varieront selon les circonstances nationales et les situations de location particulières. Les candidats potentiels peuvent être les propriétaires de l'immeuble, ses gestionnaires, une société de gestion ou un prestataire de services délégués, des associations de propriétaires, etc. ».*

Au vu des risques qui peuvent se poser pour la protection de la vie privée[59], la Commission nationale considère que les situations dans lesquelles cette charge incombe aux propriétaires - à supposer que ces dernières reflètent en pratique la réalité du contexte juridique au niveau national - devraient rester exceptionnelles.

17. En ce qui concerne la note d'information visée à l'article 11.3 du projet de loi, les informations minimales devant y figurer sont énumérées à l'article 7.2 du projet de règlement grand-ducal, dont notamment la comparaison de la consommation énergétique actuelle avec *« la consommation de l'unité privative pour la même période au cours de l'année précédente (…) ».* Il en résulte que cette comparaison est susceptible de contenir des informations se rapportant à un tiers, à savoir l'occupant précédent de l'unité privative.

La CNPD émet des doutes quant à la conformité de cette disposition à la directive 2012/27/UE telle que modifiée par la directive (UE) 2018/2002. Selon le point 3.c) de l'annexe VII *bis* de cette directive, les États membres veillent à ce que les utilisateurs finals disposent de *« la comparaison de la consommation énergétique actuelle de l'utilisateur final avec sa consommation pour la même période au cours de l'année précédente (…). »* La recommandation (UE) 2019/1660, dans son point 9.3.1., est formelle : *« Compte tenu des exigences en termes de protection des données et de vie privée (voir également le point 7.5), cette exigence doit être interprétée comme s'appliquant uniquement aux informations relatives à l'énergie consommée par l'occupant actuel, à savoir le même utilisateur final que celui qui doit pouvoir accéder aux informations ».* Partant, l'article 7.2.3°a) du projet de règlement grand-ducal risque d'être contraire tant à la directive 2012/27/UE telle que modifiée par la directive (UE) 2018/2002 qu'au principe de minimisation des données consacré à l'article 5.1.c) du RGPD.

18. De même, l'article 7.2.3°b) du projet de règlement grand-ducal est susceptible

[58] Article 10bis.3 de la directive 2012/27/UE relative à l'efficacité énergétique telle que modifiée par la directive 2018/2002 du Parlement européen et du Conseil du 11 décembre 2018.
[59] Cf. point 5 du présent avis.

ANNEXES

de ne pas respecter l'esprit du texte européen de référence tout en soulevant des problématiques liées à la protection des données personnelles. Ledit article prévoit une possibilité de comparaison de consommation de l'utilisateur de l'unité privative avec *« la consommation d'un utilisateur final de référence déterminée sur base de la consommation moyenne des unités privatives de l'immeuble bâti concerné ».* À supposer qu'un immeuble bâti de taille restreinte soit concerné, par exemple un immeuble qui comporterait deux unités privatives, et que la moyenne de consommation de cet immeuble soit ensuite transmise à l'utilisateur final, alors ce dernier pourrait aisément en déduire, de manière indirecte, la consommation du/des autre(s) occupant(s) de la seconde unité privative concernée.

19. L'article 11.3, alinéas 2 et 3, du projet de loi sous examen prévoit, quant à lui, la procédure à suivre pour la transmission de la note d'information en cas de copropriété. Ainsi en pareil cas, le syndic transmet cette dernière aux copropriétaires qui eux-mêmes la feront suivre auprès des locataires des unités privatives concernées, en d'autres termes les occupants.

Comme soulevé au point 16 ci-avant, la CNPD est d'avis que les cas dans lesquels il incombe aux propriétaires de fournir les informations aux utilisateurs finals sans contrat direct ou individuel avec un fournisseur d'énergie - à supposer que cette dernière situation reflète en pratique la réalité du contexte juridique au niveau national - doivent, dans la mesure du possible, rester un cas d'exception. En l'absence de toute précision des finalités du traitement par le projet de loi, il existe par ailleurs un risque accru de réutilisation des données de consommation des locataires par le propriétaire pour des finalités incompatibles avec celles prévues par la directive (UE) 2018/2022[60].

20. En outre, la CNPD se demande si le fait de prévoir que le syndic transmette la note d'information aux copropriétaires qui, quant à eux, la feront suivre auprès des occupants ne serait pas susceptible de rentrer en contradiction avec les termes de l'article 2.3 du projet de loi. Tout en renvoyant à l'article 11, l'article 2.3 du projet de loi précise qu'en cas de copropriété, il appartient aux syndics, et non aux copropriétaires, de mettre à disposition les données et informations relatives à la facturation et à la consommation. Aux yeux de la Commission nationale, le projet de loi présente une certaine ambiguïté quant à la personne chargée, en cas de copropriété, de la communication des données de consommation aux locataires et, par conséquent, quant à la détermination du responsable de traitement et des obligations qui découlent de cette qualification.

Afin de limiter le nombre d'acteurs ayant accès aux données de consommation et d'éviter toute potentielle discordance du texte, la CNPD se demande ainsi s'il ne serait pas plutôt envisageable de prévoir uniformément dans le texte que le syndic transmette lui-même directement la note

[60] Cf. point 12 du présent avis.

d'information auprès de l'occupant final concerné, comme cela est d'ailleurs aussi le cas pour la note d'évaluation visée par l'article 11.2 du projet de loi.

21. D'après le tableau de concordance du projet de loi, l'article 11.4, alinéa 1er, du projet de loi transpose l'article 10bis.2.d) de la version consolidée de la directive 2012/27/UE qui prévoit que *« [l]es États membres promeuvent la cybersécurité et garantissent la protection des données et de la vie privée des utilisateurs finals conformément aux dispositions applicables du droit de l'Union »*. La recommandation (UE) 2019/1660 précise, quant à elle, en son point 7.5 intitulé « Disponibilité des données et vie privée », dernier paragraphe, que *« [s]i cette disposition [i.e. l'article 10bis.2.d) précité] n'ajoute aucune obligation spécifique au-delà de celles déjà applicables au titre du droit de l'Union (comme le règlement général sur la protection des données), elle souligne que la cybersécurité, le respect de la vie privée et la protection des données sont des questions qui s'appliquent aussi au contexte des mesures, du comptage divisionnaire, de la lecture à distance et de la facturation de l'énergie thermique »*.

22. À la lecture de l'article 11.4, alinéa 1er, du projet de loi, force est d'abord de constater que seule la mention d'un espace personnel « sécurisé » sur internet est prévue sans aucune autre indication complémentaire à cet effet, notamment en ce qui concerne la personne ou l'entité chargée de sa mise en place ou en ce qui concerne les mesures de sécurité. La CNPD comprend ensuite qu'en renvoyant au paragraphe 2, les auteurs du projet de loi entendent également conférer la possibilité d'opter pour ce moyen de communication électronique aux occupants des unités privatives recevant les informations de consommation par le propriétaire ou le syndic. Se pose dès lors la question de savoir dans les cas où les occupants ne seraient pas directement liés contractuellement avec le fournisseur d'énergie - à supposer cette situation juridique encore existante au niveau national - s'il appartient au syndic, voire au propriétaire, de mettre en place une telle plateforme en ligne, ce qui constituerait une charge considérable.

Dans les commentaires de l'article 11 du projet de loi, il est indiqué que la formulation *« par le biais d'un espace personnel sécurisé sur internet »* a été empruntée au Code de l'énergie français, et plus spécifiquement à l'article L741-2 de ce dernier. Or ce même article règle la mise à disposition des factures sur un support durable autre que le papier, notamment par le biais d'un espace sécurisé en ligne. Celle-ci est assurée par le fournisseur dans le cadre d'un contrat d'abonnement à un réseau de chaleur et de froid auprès de son abonné qui doit lui-même en être également informé. Cette relation contractuelle telle que visée par le texte français est donc distincte de celle dans laquelle l'occupant qui, n'étant pas le client final, reçoit les informations relatives à sa consommation de la part du syndic ou du propriétaire - à supposer cette situation exceptionnelle encore existante au niveau national - d'où l'interrogation de la CNPD quant au renvoi, dans l'article, 11.4, alinéa 1er, au paragraphe 2 de l'article 11.

23. De plus, la Commission nationale s'interroge sur l'étendue des informations visées par cet espace et a fortiori le type

ANNEXES

de données personnelles concernées. À la lecture de l'article 11.4 du projet de loi, il semble que la note d'information telle que mentionnée par l'article 11.3 ne soit pas incluse. Dès lors, la facture et la note d'évaluation seraient-elles bien les seules concernées par cet espace sécurisé ? La CNPD est d'avis que la mise à disposition des informations en ligne mériterait plus de précision par les auteurs du projet de loi.

24. Quand bien même aucune obligation spécifique en matière de protection des données ne serait ajoutée par la directive à transposer, la recommandation (UE) 2019/1660 rappelle tout de même l'importance du respect des dispositions déjà en vigueur comme le RGPD.

Or, il semble que le projet de loi ne satisfait pas aux exigences liées à l'application des règles du RGPD, en particulier aux prescriptions de l'article 6.3. En l'espèce, le traitement des données de consommation serait nécessaire au respect d'une obligation légale créée par le projet de loi sous avis, conformément à l'article 6.1.c) du RGPD. L'article 6.3 du RGPD qui concerne spécifiquement ce fondement prévoit que *« les finalités du traitement sont définies dans cette base juridique »* et que des dispositions spécifiques peuvent être incluses *« 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; […] »*. La CNPD regrette que le projet de loi ne contienne pas de telles dispositions[61].

25. La Commission nationale note finalement que certaines législations d'autres États membres en matière énergétique insistent particulièrement sur l'importance de la protection des données, comme le décret belge wallon du 15 octobre 2020 relatif à l'organisation du marché de l'énergie thermique et aux réseaux d'énergie thermique[62] qui prévoit une section 2 entièrement dédiée à la protection de la vie privée. Cette dernière qualifie notamment les différents acteurs en cause en fonction des traitements et rappelle l'importance du respect des finalités retenues et de la durée de conservation limitée.

Ainsi adopté à Belvaux
en date du 23 février 2024.

Pour la Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[61] Cf. points 6, 10 et 12 du présent avis.
[62] https://wallex.wallonie.be/eli/loi-decret/2020/10/15/2020204339

6

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8355 portant modification 1° de la loi électorale modifiée du 18 février 2003 et 2° de la loi modifiée du 16 juin 2017 sur l'organisation du Conseil d'État

Délibération n°16/AV6/2024
du 8 mars 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement 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 (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

2. Par courrier en date du 21 février 2024, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer sur le projet de loi portant modification 1° de la loi électorale modifiée du 18 février 2003 et 2° de la loi modifiée du 16 juin 2017 sur l'organisation du Conseil d'État (ci-après le « projet de loi »).

3. Il ressort de l'exposé des motifs que le projet de loi sous examen a pour objectif principal de simplifier la procédure d'échange entre États membres de l'Union européenne des données des ressortissants des autres États membres, électeurs aux élections européennes dans une commune luxembourgeoise. En vue des prochaines élections européennes qui auront lieu le 9 juin 2024, le projet de loi sous avis propose également de simplifier certaines procédures dans l'intérêt des acteurs impliqués dans l'organisation et le déroulement des élections, et de préciser certaines dispositions pour en améliorer la sécurité juridique.

4. La Commission nationale formulera dans le présent avis ses observations quant aux problématiques relatives à la protection des données à caractère personnel soulevées par le projet de loi.

I. Sur l'échange des données électorales entre les États membres de l'Union européenne (Art. 1er du projet de loi)

5. L'article 1er du projet de loi sous avis concerne la procédure d'échange de données entre les États membres de l'Union européenne dans le cadre des élections européennes afin d'éviter le double vote et la double candidature, tel que prévu à l'article 9 de la loi électorale modifiée du 18

ANNEXES

février 2003. Le projet de loi vise à simplifier cette procédure en désignant le Centre des technologies de l'Information de l'État (ci-après le « CTIE »), à la place des collèges des bourgmestre et échevins de chaque commune, comme autorité en charge de l'établissement et de la transmission d'une liste qui contient les données des ressortissants des autres États membres de l'Union européenne, inscrits sur les listes électorales. Il transmet cette liste au ministre ayant les Affaires étrangères dans ses attributions (ci-après le « ministre ») qui informe les États membres d'origine respectifs des électeurs inscrits.

6. Ainsi, le projet de loi sous examen instaure une obligation légale de traiter un certain nombre de données à caractère personnel. La CNPD constate que l'établissement et la transmission de la liste contenant les données électorales trouvent leur base de licéité dans l'article 6.1.c) du RGPD en vertu duquel le traitement est licite s'il est *« nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ».* Dans ce cas de figure, l'article 6.3 du RGPD prévoit une contrainte particulière liée à la licéité du traitement dans la mesure où le fondement et les finalités du traitement doivent être définies soit par le droit de l'Union européenne, soit par le droit national. De plus, cette base juridique doit répondre à un objectif d'intérêt public et être proportionné à l'objectif légitime poursuivi.

7. En effet, la finalité du traitement est définie à l'article 13 de la Directive 93/109/CE du Conseil du 6 décembre 1993 fixant les modalités de l'exercice du droit de vote et d'éligibilité aux élections au Parlement européen pour les citoyens de l'Union résidant dans un État membre dont ils ne sont pas ressortissants, qui dispose que *« [l]es États membres échangent les informations nécessaires à la mise en œuvre de l'article 4 [interdisant le double vote et la double candidature]. À cette fin, l'État membre de résidence transmet, sur la base de la déclaration formelle visée aux articles 9 et 10, à l'État membre d'origine, dans un délai approprié avant chaque scrutin, les informations relatives aux ressortissants de ce dernier inscrits sur les listes électorales ou ayant présenté une candidature. L'État membre d'origine prend, en conformité avec sa législation nationale, les mesures appropriées afin d'éviter le double vote et la double candidature de ses ressortissants. »*

1) <u>Les catégories de données</u>

8. Conformément à l'article 5.1.c) du RGPD, seules les données adéquates, pertinentes et nécessaires au regard des finalités poursuivies par le responsable du traitement doivent être collectées et traitées (principe de minimisation des données). En l'espèce, il s'agit des données relatives aux ressortissants d'autres États membres de l'Union européenne qui sont électeurs aux élections européennes dans une commune luxembourgeoise. Cependant, l'article 1er du projet de loi prévoit que le CTIE établit cette liste *« sur base des données contenues dans le registre national des personnes physiques au sens de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques »* sans pour autant préciser de quelles catégories de données il s'agit concrètement.

9. De ce fait, la CNPD se demande si la liste élaborée par le CTIE contient toutes les données personnelles contenues dans le registre national des personnes physiques (ci-après le « RNPP »), telles qu'énumérées dans l'article 5 de la loi susmentionnée. La liste établie par le CTIE devrait se limiter aux seules données nécessaires au regard des finalités pour lesquelles elles sont traitées, telles que le nom, le prénom et la date de naissance des électeurs inscrits sur les listes électorales, ceci en application du principe de minimisation prévu à l'article 5.1.c) du RGPD.[63]

10. Par ailleurs, la Commission nationale tient à souligner que le traitement des données à caractère personnel relève d'une matière réservée à la loi en vertu des articles 31 et 37 de la Constitution. Ainsi, il est d'autant plus regrettable que le texte du projet de loi, en se référant à une liste établie *« sur base des données contenues dans le [RNPP] »*, reste vague et indéfini quant aux catégories de données qui seront contenues dans cette liste. La CNPD recommande vivement que le texte du projet de loi énumère de manière exhaustive les catégories de données susceptibles d'y figurer, tout en veillant à respecter le principe de minimisation des données.

2) <u>Les autorités en charge</u>

11. Dans le but de soulager le collège du bourgmestre et échevins de chaque commune, le projet de loi entend désigner le CTIE comme l'autorité en charge de l'établissement de la liste, triée par nationalité, de tous les ressortissants des autres États membres de l'Union européenne, électeurs aux élections européennes, et de la transmission de cette liste au ministre.

12. La CNPD en déduit que le CTIE est le responsable du traitement pour l'établissement de la liste et sa transmission subséquente au ministre. De même, le ministre est, en principe, à considérer comme responsable du traitement consistant à transmettre les informations de ladite liste aux États membres d'origine respectifs des électeurs inscrits. Selon la compréhension de la CNPD, il s'agit de deux responsables indépendants et successifs et non pas de responsables conjoints du traitement.

13. Cependant, la CNPD note une certaine incohérence entre le texte du projet de loi et le commentaire des articles. En effet, selon le commentaire de l'article 1er, *« l'échange de ces listes parmi les États membres est effectuée via une plateforme électronique mise en place et gérée par l'Union européenne et dont le gestionnaire au niveau national constitue le Centre [CTIE] et le ministre ayant les Affaires étrangères dans ses attributions »*. La Commission nationale se pose la question de savoir qui est effectivement compétent pour transmettre la liste contenant les données électorales aux autres États membres et s'il existe une éventuelle responsabilité conjointe. En plus, il semble ressortir de la fiche d'évaluation d'impact que le CTIE serait en charge de la transmission de ladite liste aux autres États membres tandis que le commentaire

[63] V. en ce sens : Avis 61.346 du Conseil d'État du 16 mai 2023, doc. parl. 8150/01, pp. 5 et 6.

ANNEXES

d'article fait mention d'une validation préalable de la liste par les communes, ce qui n'est cependant pas prévu par le texte du projet de loi.

14. Par conséquent, la CNPD se permet de rappeler que la notion de responsable du traitement joue un rôle important dans l'application du RGPD dans la mesure où elle détermine qui est responsable des différentes règles en matière de protection des données ainsi que la manière dont les personnes concernées peuvent exercer leurs droits.[64] Il est encore à noter que la notion de responsable (conjoint) du traitement est une notion fonctionnelle en ce qu'elle vise à répartir les responsabilités en fonction des rôles réels joués par les parties.[65] Ainsi, les dispositions du projet de loi devraient néanmoins refléter la réalité des activités exercées par les différents acteurs et donner, de cette manière, des indications suffisamment claires quant à l'entité qui est à considérer comme responsable du traitement.

II. <u>Sur l'abandon de l'envoi d'une liste comportant les données relatives aux électeurs en tutelle (Art. 7 du projet de loi)</u>

15. À l'heure actuelle, l'article 89, alinéa 3, de la loi électorale modifiée du 18 février 2003 prévoit que le préposé du répertoire civil auprès du Parquet Général envoie une liste comportant des données relatives aux électeurs en tutelle aux collèges des bourgmestre et échevins des communes de résidence des majeurs en tutelle en vue de la remettre par la suite aux bureaux de vote principaux. La CNPD salue que le projet de loi propose de supprimer l'envoi d'une telle liste comportant des données personnelles relatives aux électeurs en tutelle, notamment des données dites « sensibles », au sens de l'article 9 du RGPD, qui ont trait à la santé de la personne concernée.

16. En effet, les auteurs du projet de loi font remarquer qu'il n'est pas nécessaire de transmettre cette liste aux collèges des bourgmestre et échevins et à destination finale des bureaux de vote principaux de sorte que la suppression de cette disposition contribue au respect du principe de minimisation de données inscrit à l'article 5.1.c) du RGPD.

III. <u>Sur l'abandon de l'obligation de renseigner la profession des présentants (Art. 9, 19 et 21 du projet de loi)</u>

17. La loi électorale modifiée du 18 février 2003 détermine les informations sur les candidats et présentants qui doivent être renseignées dans la liste des candidats lors du dépôt. La Commission nationale se félicite que le projet de loi propose d'abandonner l'obligation de renseigner la profession des présentants sur cette liste dans le cadre des élections législatives, communales et européennes (Art. 9, 19 et 21 du projet de loi). Les auteurs indiquent à bon droit dans le

[64] V. en ce sens: Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p.3, disponibles sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr.
[65] *Ibid.*, p.4.

commentaire des articles qu'il n'y a dans ce contexte aucun intérêt d'inclure cette donnée personnelle et qu'il s'agit de limiter au strict nécessaire les informations à renseigner sur ladite liste.

18. La CNPD se permet simplement de rappeler l'importance du principe de minimisation des données consacré à l'article 5.1.c) du RGPD. À cet égard, elle constate que les informations devant être renseignées sur les listes des candidats lors du dépôt ne sont pas les mêmes selon qu'il s'agit des élections législatives, communales ou européennes, sans qu'elle soit toutefois en mesure d'identifier une raison justifiant cette différence de traitement. À titre d'exemple, dans le cadre des élections législatives, la liste doit comprendre le sexe des présentants, alors que tel n'est pas le cas pour les élections communales ou européennes. La Commission nationale invite dès lors les auteurs du projet de loi de reconsidérer pour chaque donnée personnelle la nécessité de la faire figurer dans les listes électorales, afin d'assurer le respect du principe de minimisation des données.

Ainsi adopté à Belvaux
en date du 8 mars 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Alain Herrmann
Commissaire

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8305 portant : 1° mise en œuvre du règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n°1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission ; 2° mise en œuvre du règlement (UE) 2022/1190 du Parlement européen et du Conseil du 6 juillet 2022 modifiant le règlement (UE) 2018/1862 en ce qui concerne l'introduction dans le système d'information Schengen (SIS) de signalements pour information concernant des ressortissants de pays tiers dans l'intérêt de l'Union ; 3° mise en œuvre de l'article 20 du règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 ; 4° mise en œuvre de l'article 20 du règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil ; 5° modification du Code de procédure pénale ; 6° modification du Code civil ; 7° modification de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ; 8° modification de la loi modifiée du 18 décembre 2015 relative à la protection internationale et à la protection temporaire ; 9° modification de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 10°modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale

Délibération n°17/AV7/2024
du 15 mars 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

De plus, conformément à l'article 8.3° de ladite loi du 1er août 2018, transposant en droit national l'article 46.1.e) de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, la CNPD *« 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 ».*

2. N'ayant pas été directement saisie par Monsieur le Ministre de la Sécurité intérieure, la Commission nationale souhaite néanmoins se prononcer quant au *projet de loi n°8305 portant : 1° mise en œuvre du règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n°1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission ; 2° mise en œuvre du règlement (UE) 2022/1190 du Parlement européen et du Conseil du 6 juillet 2022 modifiant le règlement (UE) 2018/1862 en ce qui concerne l'introduction dans le système d'information Schengen (SIS) de signalements pour information concernant des ressortissants de pays tiers dans l'intérêt de l'Union ; 3° mise en œuvre de l'article 20 du règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 ; 4° mise en œuvre de l'article 20 du règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil ; 5° modification du Code de procédure pénale ; 6° modification du Code civil ; 7° modification de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration ; 8° modification de la loi modifiée du 18 décembre 2015 relative à la protection internationale et à la protection temporaire ; 9° modification de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 10°modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale* (ci-après le « projet de loi »).

3. Le système d'information Schengen (ci-après le « SIS ») est un système informatique européen à grande échelle facilitant le partage d'informations entre autorités compétentes des États membres

ANNEXES

participants. Il compense notamment *« la suppression des contrôles aux frontières et constitue l'outil de coopération le plus efficace pour les autorités compétentes en matière de frontières et d'immigration ainsi que pour les autorités policières, douanières et judiciaires de l'UE et des pays associés à l'espace Schengen »*[66]. En date du 31 décembre 2022, le SIS contenait 86.461.806 signalements[67]. Ce système informatique à grande échelle contient dès lors une grande masse de données à caractère personnel.

4. La refonte dans laquelle s'inscrit le projet de loi sous avis est la deuxième grande réformation du système depuis son entrée en opération en 1995. En effet, le règlement modifié (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n°1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (ci-après le « règlement SIS »), vise à moderniser le fonctionnement et l'utilisation du SIS.

5. Selon l'exposé des motifs, le projet de loi entend assurer le bon fonctionnement du nouveau cadre européen du SIS en introduisant dans la législation luxembourgeoise des dispositions propres au fonctionnement national dans le contexte du SIS, y compris dans le domaine de la protection des données.

6. Il convient encore de soulever que le règlement SIS[68] oblige la CNPD à effectuer des audits réguliers des activités de traitement des données dans le cadre du N.SIS, c'est-à-dire de la copie nationale partielle de la base de données du SIS, et de contrôler la licéité du traitement des données à caractère personnel dans le SIS sur le territoire luxembourgeois.

7. Dans ce contexte, la CNPD tient à faire part de ses observations par rapport à certains articles du projet de loi et du règlement SIS présentant des aspects ayant trait à la protection des données à caractère personnel.

8. Enfin, la fiche d'impact indique que *« [l]e texte du projet de loi a été élaboré en concertation avec les parties citées ci-avant »* et que la CNPD figure parmi les parties citées. Elle souhaite néanmoins soulever que bien qu'une sorte de concertation ait eu lieu au stade de l'avant-projet de loi, elle n'a néanmoins pas pu se prononcer ni sur la version finale du texte, ni sur l'entièreté du texte. Il ne saurait être déduit de cette concertation que le texte final du projet de loi ait été approuvé par la CNPD.

V. Concernant les articles 2 et 3 du projet de loi

[66] Voir site de la Commission européenne au sujet du SIS ; https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_fr.
[67] Voir les statistiques annuelles sur SIS d'eu-LISA de 2022, p.10 ;
[68] Voir article 69 du règlement SIS.

9. La CNPD s'interroge quant à savoir si les auteurs du projet de loi ont anticipé l'application du texte de loi au regard de la protection des données en s'interrogeant sur la responsabilité des différents acteurs, et en particulier sur la ou les entité(s) endossant les rôles de responsable(s) du traitement et de sous-traitant et, le cas échéant, de responsable conjoint du traitement.

10. La notion de responsable du traitement joue un rôle important dans la mesure où elle détermine qui est responsable des différentes règles en matière de protection des données ainsi que la manière dont les personnes concernées peuvent exercer leurs droits[69]. Il est encore à noter que la notion de responsable (conjoint) du traitement est une notion fonctionnelle en ce qu'elle vise à répartir les responsabilités en fonction des rôles réels joués par les parties[70].

11. L'identité du ou des responsable(s) du traitement ne ressort pas du texte de projet de loi dans sa rédaction actuelle. Par conséquent, la Commission nationale n'est pas en mesure d'apprécier les responsabilités en matière de protection des données. La CNPD estime indispensable que les auteurs du projet de loi identifient ce(s) dernier(s). En ce sens, elle ne peut que conseiller aux auteurs du projet de loi d'établir une cartographie des flux de données.

12. Considérant les éléments susmentionnés, la CNPD constate que le règlement SIS prévoit la désignation de deux autorités qui jouent un rôle central dans le traitement de données à caractère personnel dans le SIS.

D'une part, l'« office N.SIS » qui a pour missions d'exploiter la copie nationale et d'assumer la responsabilité centrale du N.SIS conformément à l'article 7 du règlement SIS. Ainsi, l'office N.SIS doit s'assurer du respect du règlement SIS, parmi lesquelles figurent également des dispositions en matière de protection des données.

D'autre part, un bureau « SIRENE » qui a pour missions d'introduire les signalements contenant les données à caractère personnel dans le SIS, de coordonner la vérification de la qualité des données à introduire et de réagir aux demandes d'informations supplémentaires.

13. A noter que le bureau SIRENE introduit les signalements pour le compte des autorités compétentes listées à l'article 5 du projet de loi. Ces dernières jouent dès lors également un rôle en matière de protection des données comme elles décident de l'introduction d'un signalement.

14. Il ressort des articles 2 et 3 du projet de loi que la Police grand-ducale assume le rôle de bureau SIRENE et d'office N.SIS. Ces rôles attribués par le règlement SIS sont à distinguer des obligations et devoirs du responsable de traitement découlant du cadre légal applicable en matière de protection des données. Par conséquent

[69] V. en ce sens: Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 3., disponibles sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr

[70] *Ibid.*, p.4.

ANNEXES

la CNPD s'interroge quant à savoir si les auteurs du projet de loi ont appréhendé l'articulation des rôles, obligations et devoirs entre le bureau SIRENE, l'office N.SIS et les autorités susceptibles de demander l'introduction d'un signalement.

15. De plus, la CNPD s'interroge concernant l'interprétation faite par les auteurs du projet de loi de la notion de « responsabilité centrale » présente tant à l'article 7.1 du règlement SIS qu'à l'article 3.1 du projet de loi ? Est-ce que cette responsabilité centrale englobe également la responsabilité concernant la conformité des traitements en matière de protection des données ? Il ressort par exemple de l'article 59.1 du règlement SIS qu'*« [u]n État membre signalant est responsable de l'exactitude et de l'actualité des données dans le SIS, ainsi que de la licéité de leur introduction et de leur conservation dans le SIS »*. La CNPD se demande quelle entité sera chargée d'assumer cette responsabilité au niveau national. Si l'office N.SIS est désigné, comment effectue-t-il ce contrôle en pratique ? La CNPD tient à rappeler qu'en l'état actuel du projet de loi, ce sont d'autres autorités qui décident de l'opportunité d'introduire un signalement ou non. Dans l'hypothèse où l'office N.SIS remettrait en question la licéité d'un signalement, comment pourrait-elle contraindre une autorité compétente à revoir sa décision ? Se pose en effet la question quant au contrôle effectif réel que sera en mesure d'effectuer les agents du bureau SIRENE et de l'office N.SIS sur les autorités désignées aux articles 4 et 5 du projet de loi. La relation hiérarchique et opérationnelle entre ces acteurs laisse subsister des doutes quant à la réelle possibilité, par exemple, de ces agents à faire observer à l'administration judicaire que ses signalements ne respectent potentiellement pas la réglementation.

16. Par ailleurs, la CNPD rappelle que, conformément au règlement SIS, chaque État membre doit désigner un ou plusieurs bureaux SIRENE qui, sur base de l'article 7.2 dudit règlement, *« coordonnent la vérification de la qualité des informations introduites dans le SIS »*. Le bureau SIRENE devra donc travailler en étroite collaboration avec l'office N.SIS qui, comme expliqué ci-dessus, endosse potentiellement la responsabilité de la qualité des informations. À ce titre, si les rédacteurs du projet de loi entendent maintenir ces deux désignations au sein de la Police grand-ducale, il sera impératif d'établir un cadre de gouvernance, afin que les agents en charge de ces missions distinguent parfaitement leurs missions relevant de leurs cadres « office N.SIS » et « bureau SIRENE ».

17. Par ailleurs, le bureau SIRENE doit, en conformité avec l'article 7.2 alinéa 2 du règlement SIS, disposer d'un accès aux fichiers nationaux. En effet, cette disposition prévoit que *« [c]haque bureau SIRENE dispose, dans le respect du droit national, d'un accès facile direct ou indirect à toutes les informations nationales pertinentes, y compris aux bases de données nationales et à toutes les informations sur les signalements de son État membre, ainsi qu'aux avis d'experts, afin d'être à même de réagir aux demandes d'informations supplémentaires rapidement et dans les délais prévus à l'article 8 »*. La CNPD se demande dès lors comment cet accès direct ou indirect est prévu au Luxembourg, considérant que le projet de loi reste muet à cet égard.

18. Enfin, la Commission nationale se rallie aux observations contenues dans l'avis du Conseil d'État[71] au regard de l'article 2.3 du projet de loi, disposition sur laquelle ce dernier a formulé une opposition formelle. En effet, selon la compréhension de la CNPD il faudrait lister la ou les autorités compétentes qui peuvent introduire des signalements en parallèle du bureau SIRENE. La CNPD se demande par ailleurs s'il ne faudrait pas clarifier quels signalements cette ou ces autorités peuvent introduire dans le SIS. Au vu des développements précédents, ces clarifications semblent essentielles pour déterminer les rôles et responsabilités respectives en matière de protection des données

VI. Concernant l'article 9 du projet de loi

19. Concernant la rédaction de l'article 9.1 du projet de loi, qui a pour objet de préciser la condition selon laquelle les données dactyloscopiques peuvent être vérifiées et l'identité de la personne établie, les auteurs ont procédé à un renvoi à l'article 40 du règlement SIS. Cet article précise que *« [c]es données dactyloscopiques consistent en des séries complètes ou incomplètes d'empreintes digitales ou d'empreintes palmaires découvertes sur les lieux d'infractions terroristes ou d'autres infractions graves faisant l'objet d'une enquête »*. Le projet de loi reste silencieux quant à la définition de ce qu'est une « infraction grave ». Une telle définition, ou du moins une délimitation, entres les « infractions simples » et les « infractions graves » semble néanmoins essentielle dans le contexte du présent projet de loi, étant donné qu'il s'agit d'un critère déterminant pour l'introduction d'un signalement dans le SIS. La CNPD se demande si la définition retenue dans le cadre du règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) 1077/2011, (UE) 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 ne pourrait pas servir d'inspiration. En effet, l'article 3.1. point 16 de ce règlement définit l'infraction pénale grave comme *« une infraction qui correspond ou est équivalente à l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI, si elle est passible, en droit national, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans »*.

20. D'autre part, la Commission nationale souhaite exprimer sa plus vive inquiétude concernant l'interprétation qu'il est possible de faire de l'article 40 du règlement SIS, en ce qu'il indique : *« Ces données ne sont introduites dans le SIS que s'il peut être établi avec un degré très élevé de probabilité qu'elles appartiennent à un auteur de l'infraction ».* En effet, le recours à la formulation « avec un degré très élevé de probabilité » implique, dans une société respectueuse de la vie privée, une analyse à priori sur base de critères d'évaluation rigoureux fixés par la loi. Sans cadre légal strict et précis, la CNPD craint que l'ensemble des données soit systématiquement intégré au SIS.

[71] Voir l'avis du Conseil d'État du 6 février 2024, doc. parl. 8305/01, p.4 et 5.

ANNEXES

21. La Commission nationale tient à souligner dans ce contexte que l'article 8 de la Convention européenne des droits de l'homme garantit le droit au respect de la vie privée et familiale. Par ailleurs, les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») accordent à toute personne le droit au respect de sa vie privée et familiale, ainsi que le droit à la protection des données personnelles la concernant. Néanmoins, ces droits fondamentaux ne sont pas des prérogatives absolues puisque la possibilité d'une ingérence ou d'une limitation est prévue tant par l'article 8.2 de la Convention européenne des droits de l'homme que par l'article 52.1 de la Charte.

C'est dans ce contexte que le respect des principes de proportionnalité et de nécessité est essentiel, car cette ingérence ou limitation peut uniquement être justifiée à condition qu'elle soit, entre autres, prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante.[72]

22. Il convient dès lors de s'interroger quant à savoir si l'absence de critères dans la loi ne s'opposerait pas aux dispositions de la Charte et de la Convention européenne des droits de l'homme. En effet, le critère de prévisibilité et d'accessibilité de la loi précité protège notamment les personnes concernées contre l'arbitraire. Si la loi prévoit les critères sur base desquelles des données personnelles peuvent être introduites dans le SIS dans le cadre d'un signalement en vertu de l'article 40 du règlement SIS, les autorités compétentes ne peuvent pas décider aléatoirement de recourir à ce type de signalement.

23. Il échet de souligner que les données dactyloscopiques visées par l'article 40 du règlement SIS sont des données relevant de catégories particulières de données à caractère personnel au sens du RGPD et de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, et qui sont soumises à un régime de traitement plus strict. En effet, l'article 9 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 autorise le traitement de telles catégories de données *« uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée ».*

24. Par ailleurs, la CNPD s'interroge sur la formulation choisie par les auteurs du projet de loi concernant la rédaction de l'article 9.2 *« tout traitement de données en vertu de l'article 40 du règlement (UE) 2018/1862 autre que l'insertion, la consultation ou la comparaison doit faire l'objet d'une autorisation des autorités judiciaires compétentes »*. Si la CNPD est

[72] Les autres conditions sont que l'ingérence soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité, respecte le contenu essentiel du droit à la protection des données et réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui. Pour une analyse plus détaillée de ces conditions, voir délibérationn°2/2021 du 4 février 2021 de la Commission nationale pour la protection des données, doc. pari. n° 7425/09, point I. 1. b).

en mesure d'appréhender la portée des mots « insertion » et « consultation » elle reste cependant dubitative au regard de l'utilisation de « comparaison » et de « tout traitement » et se demande quels sont les traitements de données effectivement visés par cette disposition. Dans ces conditions, la CNPD se demande si l'article ne devrait pas être précisé davantage afin d'assurer une plus grande sécurité des libertés fondamentales des personnes concernées en s'attardant à définir plus précisément le cadre dans lequel les données de ces personnes sont traitées.

VII. <u>Concernant l'article 10 du projet de loi</u>

25. Dans la mesure où l'article 10 du projet de loi prévoit des dispositions relatives au régime de protection des données applicable, il doit être lu ensemble avec les articles 66 et 67 du règlement SIS.

26. L'article 66 du règlement SIS détermine les régimes de protection des données applicables. Ainsi, cet article dispose que la directive (UE) 2016/680 est applicable aux traitements de données à caractère personnel effectués dans le cadre du SIS et à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces par les autorités compétentes. La CNPD tient à faire remarquer que, selon sa compréhension, l'article 66 doit s'interpréter comme définissant un régime applicable en fonction de la finalité du traitement de données. En effet, l'article 66.2 précise que *« [l]a directive (UE) 2016/680 s'applique aux traitements de données à caractère personnel effectués, au titre du présent règlement, par les autorités et les services nationaux compétents à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. » Cette formulation « par les autorités et les services nationaux compétents »* doit s'entendre comme désignant les autorités et les services nationaux compétents dans le cadre du règlement SIS. Ainsi, toutes les autorités opérant sous le SIS appliqueraient le régime prévu par la directive (UE) 2016/680 pour autant qu'elles agissent dans le cadre du SIS et pour une finalité de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

27. Les traitements à caractère personnel effectués à d'autres fins (par exemple : pour une finalité administrative) tombent sous le régime du RGPD. Les agences européennes, à savoir eu-LISA, Frontex et Europol, doivent appliquer leur régime européen respectif.

28. L'article 67 du règlement SIS quant à lui prévoit des dispositions spécifiques sur les droits d'accès, de rectification et d'effacement des personnes concernées. Cet article doit être vu comme une lex specialis aux regard des régimes généraux cités par l'article 66 du règlement SIS.

Dans la mesure où l'article 66 du règlement SIS détermine les régimes applicables, la CNPD s'interroge sur l'utilité des

ANNEXES

paragraphes 1 et 2 alinéa 1er de l'article 10 du projet de loi. Ne serait-il pas suffisant de simplement préciser que le régime de protection des données visé à l'article 66.2 du règlement SIS est mis en œuvre au plan national par la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale ?

Dans tous les cas, l'article 10.1 et 2 en sa rédaction actuelle semble contraire au règlement SIS en ce qu'il soumet tous les traitements effectués dans le contexte SIS à la directive (UE) 2016/680 avec pour seule exception les traitements effectués par les autorités administratives à des fins administratives. Or, selon la compréhension de la CNPD, le règlement distingue les régimes applicables aux traitements effectués dans le contexte SIS en fonction de la finalité poursuivie tel que décrit aux points 26 et 27 du présent avis. Une disposition nationale qui aurait pour effet de modifier les régimes applicables serait contraire au droit de l'Union européenne.

29. Ensuite, l'article 10.2 en son deuxième alinéa dispose, conformément à l'article 66 et 67 du règlement SIS, qu'il est possible pour les autorités nationales administratives de limiter entièrement ou partiellement le droit d'accès, prévu à l'article 15 du RGPD, de la personne concernée.

30. Néanmoins, la Commission nationale souhaiterait attirer l'attention des rédacteurs du projet de loi concernant l'article 67 du règlement SIS qui précise qu'une telle limitation ne peut se faire que *« conformément au droit national, dès lors et aussi longtemps qu'une limitation partielle ou complète de cette nature constitut une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne concernée […] ».* La CNPD considère dès lors que conformément au principe de prévisibilité de la loi exigé tant par l'article 52 de la Charte que de l'article 8.2 de la Convention européenne des droits de l'homme, la loi devrait fixer les critères et conditions permettant aux autorités nationales de décider de la limitation. En effet, il pourrait être envisagé de limiter les droits par exemple en fonction de la source des données ou du type de signalement. En l'absence de disposition nationale prise en adéquation avec les garanties exigées par l'article 67 du règlement SIS, la CNPD se demande si le cadre légal envisagé est conforme au droit de l'Union.

VIII. <u>Concernant l'article 11 du projet de loi</u>

31. Les modifications prévues concernant l'article 45 du Code de procédure pénale sont susceptibles, selon la CNPD, de se révéler disproportionnées. La suppression de l'alinéa 2 du paragraphe 6, qui limitait la collecte de données personnelles sensibles à des fins déterminées, prive les personnes concernées de la sécurité dont elles disposent au regard de leur vie privée. Sans cadre ou liste exhaustive et au regard de l'ajout du nouvel alinéa 5 disposant que *« [l]es données à caractère personnel ainsi collectées peuvent être comparées avec les informations contenues dans les traitements de données à caractère personnel disponibles à la Police grand-ducale dans l'exercice de ses missions »*

la CNPD s'inquiète que soient opérés des prélèvements systématiques ou, si occasionnels, selon des critères subjectifs. Ce faisant et sur ce point, la CNPD se rallie aux conclusions du Conseil d'État et recommande l'annulation de la suppression du paragraphe en question.

32. Concernant la suppression et le remplacement du paragraphe 8 de l'article 45 du Code de procédure pénale par le paragraphe suivant *« (8) Le procès-verbal d'identification et toutes les pièces s'y rapportant peuvent être conservés pendant un délai maximal de six mois. Les empreintes digitales et les photographies recueillies en application du présent article peuvent être traitées ultérieurement par la police à des fins de prévention, de recherche et de constatation des infractions pénales si la personne contrôlée fait l'objet d'une enquête judiciaire ou mesure d'exécution endéans cette période. Les délais de conservation sont ceux applicables aux autres données à caractère personnel collectées dans le cadre de ces procédures »*, la CNPD estime que la dernière phrase génère une incertitude quant à la durée de conservation à retenir. La Commission nationale recommande donc aux auteurs du projet de loi d'adopter une formulation qui permettrait, conformément au principe de prévisibilité de la loi exigé tant par l'article 52 de la Charte que de l'article 8.2 de la Convention européenne des droits de l'homme, de comprendre plus aisément cette disposition et ainsi de diminuer l'insécurité juridique que cette disposition est susceptible de générer.

33. Par ailleurs, même si la CNPD comprend la logique sous-jacente concernant la conservation de données personnelles d'individus inconnus des services de police, la Commission nationale n'est toutefois pas en mesure d'apprécier la durée de 6 mois retenue par les auteurs du projet de loi car cette dernière n'est pas motivée. Par conséquent, elle rappelle que la durée de conservation doit être adaptée aux finalités poursuivies ainsi que adéquates et proportionnées au fonctionnement d'une société démocratique.

34. La CNPD constate au surplus, que l'article 11 du projet de loi vise à mettre en application, selon le commentaire des articles, les articles 20 paragraphes 1,2,4 et 6 du règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration. Force est de constater que l'article 11, en sa rédaction actuelle, ne vise pas expressément les paragraphes 4 et 6 dudit règlement. Par conséquent la CNPD ne comprend pas de quelle manière ces dispositions peuvent s'appliquer.

35. D'autre part, les auteurs du projet de loi, dans leur commentaire de l'article 11 arguent que *« [b]ien que ces événements [catastrophe naturelle ou accident] ne relèvent pas forcément du domaine pénal, en pratique les circonstances de ces derniers ne sont souvent pas assez claires pour exclure des infractions pénales ou d'identifier les auteurs et victimes, de sorte que les autorités judiciaires sont dans tous ces cas saisies de l'affaire. Ainsi l'article 45 du Code de procédure pénale s'applique, alors que la personne concernée est dans l'impossibilité de prouver son identité ou*

ANNEXES

de coopérer. » La CNPD s'interroge sur l'opportunité de procéder à un renvoi à l'article 45 du Code de procédure pénale. Selon sa compréhension, cet article ne peut s'appliquer que dans des cas bien précis lors d'une enquête pénale. Le paragraphe 1 de l'article 45 du Code de procédure pénale, qui ne fait pas l'objet d'une modification par les auteurs du projet de loi, délimite de manière précise les situations dans lesquelles il est applicable. Les auteurs du projet de loi n'ayant pas opéré un renvoi au règlement 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et n'ayant pas modifié en conséquence l'article 45 du Code de procédure pénale, la CNPD reste dubitative quant à cette interprétation opérée par les auteurs et se questionne sur l'opportunité d'inscrire ces moyens d'actions, concernant les catastrophes naturelles et les accidents, au sein de la loi du 18 juillet 2018 sur la Police grand-ducale.

36. La CNPD tient à préciser que la mise en application des articles 20 paragraphes 4 et 6 du règlement 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration nécessite une attention particulière car il incombe à la loi nationale d'adopter les procédures, conditions et critères selon lesquels il est possible d'interroger le CIR (c'est-à-dire le répertoire commun de données d'identité établi par l'article 17, paragraphe 1, du règlement (UE) 2019/818).

IX. <u>Concernant l'article 16 du projet de loi</u>

37. Da la même manière le projet de loi prévoit une modification de l'article 5 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale en son paragraphe 7 et dispose : *« Les délais de conservation sont ceux applicables aux données à caractère personnel dans les fichiers de la Police prévus aux articles 43quater et 43quinquies. »*

38. La CNPD conseille ici aussi aux auteurs du projet de loi d'adopter une formulation qui permettrait, conformément au principe de prévisibilité de la loi exigé tant par l'article 52 de la Charte que de l'article 8.2 de la Convention européenne des droits de l'homme, d'indiquer clairement la durée de conservation afin d'éviter toute forme d'insécurité juridique et de garantir une meilleure lisibilité pour le citoyen. Au surplus, la CNPD n'est pas en mesure d'apprécier l'opportunité de telles durées de conservation puisque ces dernières ne sont pas motivées.

La CNPD observe d'autre part, que le commentaire de l'article 16 précise que les modifications dudit article *« sont le corollaire des modifications apportées à l'article 45 du CPP dans le cadre de la mise en œuvre des articles 20 des règlements (UE) 2019/818 et (UE) 2019/817 relatifs à l'interopérabilité des bases de données européennes. »*. La Commission nationale ne peut que constater l'absence de retranscription, dans l'article 16, des paragraphes 4 et 6 dudit règlement. La CNPD attire donc l'attention des auteurs du projet de loi sur le fait que le commentaire des articles ne reflète donc pas la rédaction actuelle du projet de loi.

X. Concernant l'article 56 et l'article 73 du règlement SIS

39. L'article 56 du règlement SIS vise spécifiquement les finalités pour lesquelles les données peuvent être utilisées. Il précise qu'une utilisation de ces données pour des finalités autres que celles prévues par le règlement constitue une utilisation abusive et qui, au regard du droit national, donne lieu à des sanctions sur base de l'article 73 du même règlement. L'article 73 dispose que le droit national doit prévoir des sanctions effectives, proportionnées et dissuasives. La CNPD ne peut que constater l'absence de telles sanctions prévues par le droit national ou, tout du moins, par le projet de loi. Par conséquent, la Commission nationale encourage fortement les auteurs du projet de loi à prévoir ces sanctions.

40. Par ailleurs, l'article 56.8 précise *« [p]our autant que le droit de l'Union ne prévoie pas de dispositions particulières, le droit de chaque État membre est applicable aux données dans son N.SIS »*. La CNPD suggère que les auteurs du projet de loi détaillent le régime applicable dans une telle situation.

XI. Concernant l'article 64 du règlement SIS

L'article 64.3 du règlement SIS prévoit que *« [l]e délai pendant lequel les données peuvent être conservées dans ces fichiers est régi par le droit national ».* La CNPD s'interroge quant à savoir si ces délais sont prévus par la loi nationale. Dans le cas où ce délai ne serait pas prévu, la CNPD ne peut qu'encourager les auteurs du projet de loi à mettre en application cette disposition du règlement.

Ainsi adopté à Belvaux
en date du 15 mars 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8253 relative aux fiches d'hébergement et portant : 1° modification de loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 2° modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ; et 3° abrogation de la loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement

Délibération n°20/AV8/2024
du 29 mars 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

2. Par ailleurs, conformément à l'article 8.3° de la loi susmentionnée du 1er août 2018, transposant en droit national l'article 46.1.c) de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, la CNPD *« 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 ».*

3. Par courrier en date du 16 juin 2023, Monsieur le Ministre du Tourisme a invité la Commission nationale à se prononcer sur le projet de loi relative aux fiches d'hébergement et portant : 1° modification de loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 2° modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ; et 3° abrogation de la loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement (ci-après le « projet de loi »).

4. Il ressort de l'exposé des motifs que le projet de loi sous examen vise à remplacer la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement, un système mis en place en 1929 et ayant connu plusieurs adaptations depuis. Les modifications proposées, issues des recommandations d'un groupe de travail composé de représentants de diverses entités telles que la direction générale du Tourisme, le Ministère de la Sécurité intérieure, la Police grand-ducale et le CTIE, visent à accroître l'efficacité du système actuel tant pour les exploitants, c'est-à-dire toute personne physique ou morale qui fournit, à titre onéreux, un service d'hébergement, que pour les destinataires de ces données, qui sont la Police grand-ducale et l'Institut national de la statistique et des études économiques du Grand-Duché de Luxembourg (ci-après le « STATEC »).
La CNPD comprend du commentaire des articles relatif à l'article 1 du projet de loi qui explique qu' « Il n'importe pas, au regard de la présente loi, si la personne exerce cette activité de manière habituelle ou non et qu'elle soit ou non tenue de disposer d'une autorisation d'établissement. Ainsi, les obligations imposées par la présente loi s'appliquent également aux personnes qui, en vertu des nouvelles dispositions en matière d'établissement (projet de loi n°7989), ne seraient pas tenues de détenir une autorisation d'établissement en raison du fait que leur activité se situe en-deçà du seuil à partir duquel une telle autorisation est exigée » que les personnes physiques qui loueraient, ne serait-ce qu'à titre occasionnel, leur logement privé par le biais d'une plateforme commerciale en ligne, devraient respecter les dispositions du projet de loi sous avis.

5. La Commission nationale a pris note du dépôt d'un projet de règlement grand-ducal portant abrogation du règlement grand-ducal du 5 août 2015 relatif aux fiches à tenir par les logeurs exploitant un service d'hébergement touristique. Ce dernier a été pris en exécution de la loi du 24 juin 2008 susmentionnée afin de préciser les modalités et les délais de la communication des fiches d'hébergement et des données, de même que le modèle de ces fiches, les indications à y apporter, le mode de conservation de celles-ci ainsi que le traitement des données par la Police grand-ducale. L'ensemble de ces questions sont désormais réglées par le projet de loi sous examen.

6. La Commission nationale formulera dans le présent avis ses observations quant aux problématiques relatives à la protection des données à caractère personnel soulevées par le projet de loi.

XII. Remarques liminaires

7. La législation actuelle impose à quiconque qui héberge une personne dans un établissement d'hébergement collectif ou d'hébergement touristique privé de remplir ou de faire remplir une fiche reprenant certaines informations des personnes hébergées et de les transmettre à certaines autorités.

8. Le système des fiches d'hébergement tient à satisfaire une double finalité. En vertu de l'article 45 de la Convention d'application de l'Accord de Schengen (ci-après la « CAAS »), le Luxembourg est tenu de prendre des mesures pour assurer que les étrangers, ressortissants de l'Union européenne et de pays tiers, qui sont hébergés dans un

ANNEXES

établissement d'hébergement touristique remplissent et signent une fiche de déclaration et justifient de leur identité. En outre, le Luxembourg est tenu par le règlement (UE) n° 692/2011 du Parlement européen et du Conseil du 6 juillet 2011 concernant les statistiques européennes sur le tourisme et abrogeant la directive 95/57/CE du Conseil de fournir à l'office statistique de la Commission européenne (EUROSTAT) des statistiques sur la fréquentation des établissements d'hébergement. Donc, l'établissement ainsi que la transmission des fiches d'hébergement aux autorités respectives couvrent des fins à la fois sécuritaires et statistiques.

9. En ce qui concerne le volet sécuritaire, la Commission nationale constate que le projet de loi sous examen prévoit une transmission non-ciblée des fiches d'hébergement pour chaque voyageur et pour chaque séjour par l'exploitant à la Police grand-ducale. Cette transmission systématique et généralisée aboutit à une centralisation massive des données à caractère personnel auprès de la Police grand-ducale, ce qui soulève des questions importantes au regard du droit à la protection des données tel que consacré tant par l'article 31 de la Constitution que par les textes supranationaux.[73] Dans ce contexte, il faut souligner qu'une transmission automatique des données personnelles des voyageurs par l'exploitant aux services de police a été abrogée dans tous nos pays voisins. En effet, ni l'Allemagne, ni la France, ni la Belgique ne connaissent actuellement une transmission systématique et généralisée des données de tous les voyageurs aux services de police.[74] En revanche, les ordres juridiques susmentionnés prévoient la conservation des fiches d'hébergement par l'exploitant lui-même pendant une durée déterminée. Si la demande lui est faite, l'exploitant ou son préposé doit mettre les données enregistrées à la disposition des agents de police de sorte que le contrôle en est possible. Au-delà, la France a limité l'accès aux données en obligeant les agents de police de fonder leur demande sur l'un des trois motifs légaux prévus par le code de l'entrée et du séjour des étrangers et du droit d'asile, à savoir aux fins de prévention des troubles à l'ordre public, d'enquêtes judiciaires et de recherche dans l'intérêt des personnes.[75]

10. Force est de constater que le système des fiches d'hébergement au Grand-Duché du Luxembourg est beaucoup plus étendu et intrusif que celui de ses pays voisins et que la centralisation des données personnelles auprès de la Police grand-ducale constitue une spécificité par rapport aux autres pays. La Commission nationale aura l'occasion de revenir à cet aspect essentiel dans la suite du présent avis.

XIII. Les responsables des différents traitements

11. Il y a lieu de rappeler que la notion de responsable du traitement joue un rôle

[73] Voir article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.
[74] En Allemagne voir §29 à §31 du Bundesmeldegesetz (BMG) vom 3. Mai 2013 ; en France voir les articles R.814-1 à R.814-3 du Code de l'entrée et du séjour des étrangers et du droit d'asile ; en Belgique voir les articles 141 à 146 de la Loi du 1er mars 2007 portant des dispositions diverses.
[75] Article R.814-1 et suivants du Code de l'entrée et du séjour des étrangers et du droit d'asile.

important en matière de protection des données. Premièrement, la détermination du responsable du traitement peut avoir des incidences sur le régime juridique applicable. En effet, les traitements de données effectués à des fins pénales ou sécuritaires par des autorités compétentes, telles que la Police grand-ducale ou le Service de renseignement de l'État (ci-après le « SRE »), 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 tandis que les autres traitements, tels que ceux effectués par les exploitants ou le STATEC, relèvent du régime de droit commun, à savoir le RGPD. Deuxièmement, la détermination du responsable du traitement permet de savoir quelle entité est responsable des différentes règles en matière de protection des données ainsi que de la manière dont les personnes concernées peuvent exercer leurs droits.[76]

12. En vertu des articles 3 et 6 du projet de loi, il appartient à l'exploitant d'établir les fiches d'hébergement et de transmettre à la Police grand-ducale ainsi qu'au STATEC les données personnelles énumérées aux annexes respectivement applicables. Il en découle que l'exploitant est le responsable du traitement pour la collecte et la transmission subséquente des données des voyageurs, par le biais des fiches d'hébergement, à la Police grand-ducale et au STATEC. De même, le STATEC, la Police grand-ducale et le SRE sont à considérer comme responsables des traitements qu'ils effectuent respectivement par la suite.

13. Par conséquent, la CNPD peut se rallier aux développements faits par les auteurs dans le commentaire de l'article 6 selon lesquels les différents acteurs ne sont pas des responsables conjoints du traitement des données à caractère personnel, mais des responsables indépendants et successifs.

XIV. La collecte des données par les exploitants

14. Le projet de loi sous examen instaure l'obligation légale pour les exploitants de traiter un certain nombre de données à caractère personnel. Ainsi, la collecte des données personnelles des voyageurs par les exploitants trouve sa base de licéité dans l'article 6.1.c) du RGPD en vertu duquel le traitement est licite s'il est *« nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis »*. Dans ce cas de figure, l'article 6.3 du RGPD prévoit une contrainte particulière liée à la licéité du traitement dans la mesure où le fondement et les finalités du traitement doivent être définies soit par le droit de l'Union européenne, soit par le droit national. De plus, cette base juridique doit répondre à un objectif d'intérêt public et être proportionné à l'objectif légitime poursuivi.

15. Il résulte en outre de l'article 6.3 ainsi que du considérant 45 du RGPD que la base

[76] V. en ce sens: Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, point 3, disponibles sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr.

ANNEXES

juridique peut contenir des dispositions spécifiques visant, entre autres, à déterminer le responsable du traitement, les personnes concernées, les catégories de données qui font l'objet du traitement et la durée de conservation.

1. L'exploitant en tant que responsable du traitement

16. Tel qu'exposé sous les points 11 à 13 du présent avis, les exploitants sont à considérer comme responsables des traitements relatifs à la collecte et la transmission des données personnelles des voyageurs. Ainsi, le respect des principes énoncés à l'article 5 du RGPD s'impose aux exploitants en tant que responsables du traitement. Le présent avis se penchera plus particulièrement sur les principes de transparence, d'une part, ainsi que sur le principe d'intégrité et de confidentialité, d'autre part.

A. Le principe de transparence

17. Le principe de transparence est consacré à l'article 5.1.a) tandis que les articles 12 à 14 du RGPD exposent les exigences pratiques relatives à l'information des personnes concernées. Ainsi, les informations visées à l'article 13 du RGPD doivent être fournies par le responsable du traitement, c'est-à-dire l'exploitant, au moment même de la collecte des données d'une manière concise, transparente, compréhensible et aisément accessibles.[77] L'exigence de compréhensibilité implique que ces informations devraient être accessibles à la majorité du public visé, et donc une traduction dans une ou plusieurs langues devrait être fournie si les personnes ciblées par le responsable du traitement parlent d'autres langues.[78]

18. Par ailleurs, l'article 13.1.e) du RGPD exige que les responsables du traitement fournissent aux personnes concernées les informations relatives aux destinataires ou aux catégories de destinataires des données à caractère personnel. En l'espèce, les personnes doivent être informées sur le fait que leurs données personnelles sont traitées par la Police grand-ducale et le cas échéant par le STATEC, conformément aux explications fournies sous les points 36 et suivants du présent avis. Afin d'assurer une information complète et uniforme de toutes les personnes concernées, il pourrait être utile que le ministère compétent mette à disposition des modèles de notices d'information qui peuvent être utilisées par tous les exploitants.

B. Le rôle du CTIE au regard du principe d'intégrité et de confidentialité

19. Le commentaire de l'article 6 du présent projet de loi précise que *« le transfert des données et informations de l'exploitant vers les autorités compétentes se fait par l'intermédiaire de la solution informatique hébergée par le CTIE qui, au regard du règlement général de protection des données aura la qualité de sous-traitant des exploitants et de la Police »*. Or, la qualification retenue par les auteurs du projet de loi soulève

[77] Article 12.1 du RGPD.
[78] Groupe de travail « Article 29 », Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, Version révisée et adoptée le 11 avril 2018, points 9 et s.

plusieurs observations de la part de la CNPD.

20. Tout d'abord, il y a lieu de rappeler que l'article 4.8) 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 »*. Or, il résulte de l'article 1.6° de la loi en projet que la solution informatique est hébergée dans l'infrastructure du CTIE pour le compte du Ministre ayant le Tourisme dans ses attributions. Ce libellé donne à croire que le CTIE agirait en tant que sous-traitant du Ministre alors que, selon la compréhension de la CNPD, ce dernier n'intervient pas dans le cadre du dispositif prévu par le projet de loi. La Commission nationale estime que les explications contenues à cet égard dans le commentaire de l'article 1er n'apportent pas les clarifications nécessaires.

21. Ensuite, conformément à l'article 28.3 du RGPD, le traitement par un sous-traitant doit être régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, conclu entre le responsable du traitement et le sous-traitant, qui doit contenir certaines clauses. Ainsi, la qualification de sous-traitant a pour conséquence que les exploitants doivent conclure avec le CTIE un contrat de sous-traitance au sens de l'article 28.3 du RGPD. La conclusion d'un tel contrat n'a toutefois pas d'incidence sur la responsabilité des exploitants en matière de protection des données. La CNPD rappelle que l'exploitant, en tant que responsable du traitement, demeure responsable de la mise en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que le traitement est effectué conformément au RGPD (article 24) et doit être en mesure de le démontrer.[79] Par conséquent, la Commission nationale s'interroge si la qualification des différents acteurs, telle qu'envisagée par les auteurs du projet de loi, est adaptée à la réalité des activités réellement exercées. À titre d'exemple, il semble difficilement concevable que les exploitants donnent une quelconque instruction au CTIE de sorte qu'il y a lieu de se demander si la qualification de responsable (conjoint) du traitement ne serait pas plus appropriée en l'espèce.

2. <u>Les personnes concernées</u>

22. Le système actuel prévoit qu'une fiche d'hébergement doit être remplie par chaque voyageur à l'exception de la personne accompagnant le voyageur et des enfants de moins de 15 ans qui sont repris sur la même fiche. De plus, l'article 1er de la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement ainsi que le règlement d'exécution, tel qu'il est en vigueur depuis le 14 août 2015, ne prévoient en effet, pour les personnes voyageant en groupe, que l'obligation d'établir une fiche pour le voyageur principal et d'indiquer sur cette fiche le nombre de voyageurs accompagnant celui-ci. Aucune donnée à caractère personnel concernant les

[79] Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, Point 41, disponible sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr.

ANNEXES

personnes « accompagnantes » n'est dès lors transmise à la Police grand-ducale.

23. Les auteurs du projet de loi sous avis veulent désormais imposer aux exploitants l'obligation d'établir une fiche d'hébergement pour chaque client âgé de 15 ans ou plus et pour chaque séjour du client. La CNPD prend note des explications des auteurs concernant les raisons pour lesquelles ils veulent élargir le cercle des personnes concernées. Selon leurs explications, le système actuel serait inefficace dans la mesure où la Police ne reçoit aucune information sur l'identité des différents membres d'un groupe et il n'est pas aisé pour l'exploitant, lorsque plusieurs personnes se présentent dans son établissement sans faire partie d'un voyage organisé, de déterminer qui est le voyageur « principal » dont il est censé relever les données et qui sont les personnes accompagnantes.

24. Sur le plan européen, l'article 45.1.a) de la CAAS exclut explicitement les conjoints ou mineurs accompagnant le voyageur principal ou les membres des groupes de voyage de l'obligation de remplir une fiche d'hébergement. Ainsi, la Commission nationale se demande s'il s'avère vraiment nécessaire d'élargir le cercle des personnes concernées en tenant compte de la disposition susmentionnée.

25. Par ailleurs, l'article 1.5° du projet de loi sous examen définit comme voyageur *« toute personne âgée de 15 ans ou plus qui loge dans un hébergement touristique pour une durée ne dépassant pas trois mois consécutifs ».* De ce fait, les mineurs de quinze à dix-huit ans ont l'obligation de remplir une fiche d'hébergement pour chaque séjour dans un hébergement touristique et leurs données personnelles sont également transmises à la Police grand-ducale.
En considérant qu'il s'agit de personnes vulnérables, la CNPD estime la transmission généralisée et systématique vers la Police grand-ducale comme étant d'autant plus problématique. Il faut noter qu'à l'égard du traitement des données à caractère personnel en matière pénale, *« des 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 ».*[80]

26. En outre, le projet de loi sous examen ne fait, contrairement à la France, aucune différence entre un voyageur de nationalité étrangère et luxembourgeoise. Ainsi, la Commission nationale s'interroge sur l'obligation de remplir les fiches d'hébergement aussi bien pour les citoyens luxembourgeois. Encore une fois, il faut souligner que l'article 45 de la CAAS ne prévoit une obligation de déclaration que pour les ressortissants étrangers logés dans un établissement d'hébergement. Il y a lieu de souligner qu'en Allemagne, un projet de loi a récemment été déposé par

[80] Considérant (50) de la directive (UE) 2016/680 du parlement européen et du conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (LED).

le Ministre de la Justice, qui vise dans son article 6 la suppression de l'obligation de remplir les fiches d'hébergement pour les ressortissants allemands, ce qui représente, selon les auteurs de ce projet de loi, une mesure importante pour réduire la charge administrative des exploitants.[81]

3. Les catégories de données

27. Les voyageurs doivent fournir sur la fiche d'hébergement les informations à caractère personnel prévues par l'annexe 1 du présent projet de loi. La Commission nationale comprend qu'il s'agit notamment du numéro de la pièce d'identité présentée par le voyageur. Selon l'article 5.2 du projet de loi sous examen, l'exploitant a l'obligation de vérifier les données qui lui sont soumises sur base de la carte d'identité ou du passeport du voyageur. À cette fin, l'exploitant peut demander au voyageur de présenter une pièce d'identité dans le seul but de vérifier les renseignements fournis par celui-ci. Il s'agit d'une obligation qui est également prévue par l'article 45.1.a) de la CAAS. La Commission nationale tient à souligner que les exploitants peuvent à juste titre demander de se faire présenter une pièce d'identité afin de vérifier les données du voyageur, mais n'ont cependant pas le droit de faire une copie du document présenté conformément au principe de minimisation prévu à l'article 5.1.c) du RGPD, qui prévoit que la collecte des données doit être limitée à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

4. La durée de conservation

28. À l'heure actuelle, les exploitants d'hébergement ont une obligation de conserver les fiches d'hébergement des voyageurs pour une durée de douze mois.[82] Le projet de loi sous examen réduit la durée de conservation en disposant que toutes les fiches d'hébergement, quel qu'en soit le support, doivent être conservées pendant une période de six mois et doivent être supprimées à l'issue de cette période. La Commission nationale accueille favorablement cette réduction de la durée de conservation et rappelle qu'en vertu du principe de limitation de la conservation consacré à l'article 5.1.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 ou traitées.

XV. La transmission des données à la Police grand-ducale

29. Selon l'exposé des motifs, l'une des principales raisons de la réforme envisagée réside dans le fait que le délai actuel de soixante-douze heures, pendant lequel la Police grand-ducale peut conserver les données transmises par les exploitants, est jugé trop court. Ainsi, toute recherche sur une personne suspecte qui apparaît plus tard dans un dossier judiciaire serait

[81] Entwurf eines Vierten Gesetzes zur Entlastung der Bürgerinnen und Bürger, der Wirtschaft sowie der Verwaltung von Bürokratie (BEG IV-E), 2024.
[82] Article 4 de la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement.

ANNEXES

impossible de sorte que l'utilisation de cet outil est quasi exclusivement limitée à la recherche de personnes signalées. Les auteurs du projet de loi invoquent que le Grand-Duché du Luxembourg pourrait dans le futur davantage être utilisé comme lieu de rencontre avant la préparation d'un attentat terroriste ou pour assurer la fuite et proposent par conséquence de porter la durée de conservation à six mois. Pourtant, la Commission nationale constate que la centralisation des données auprès de la Police grand-ducale telle qu'elle est prévue dans le projet de loi sous examen et telle qu'elle existe déjà à l'heure actuelle représente une singularité par rapport à nos pays voisins.[83]

30. En effet, il existe actuellement au Grand-Duché du Luxembourg un système hybride. Les données des fiches d'hébergements de tous les voyageurs doivent être transmises dans un délai maximal de douze heures par les exploitants à la Police grand-ducale et parallèlement les originaux des fiches d'hébergement sont conservés par l'exploitant lui-même. Dans ce deuxième cas de figure, ces fiches doivent être présentées à toute réquisition aux agents de la Police grand-ducale.[84] Dès lors, le projet de loi sous examen prévoit explicitement dans son article 8.1 que *« les originaux des fiches d'hébergement établies sur support papier sont conservés par l'exploitant pendant une durée de six mois et doivent être présentés à toute demande de la Police grand-ducale »*. Ainsi, les auteurs du projet de loi souhaitent désormais donner aux agents de police la possibilité de procéder à la réquisition des fiches d'hébergement auprès de l'exploitant pendant un délai de six mois, ce qui représente la procédure commune de nos pays voisins.

31. Compte tenu du fait que le projet de loi sous examen prévoit la possibilité de procéder à cette réquisition des fiches d'hébergement auprès de l'exploitant, la Commission nationale s'interroge sur la nécessité de la transmission automatique des données à la Police grand-ducale. Dans son avis du 12 décembre 2023, le Conseil d'État s'oppose formellement à cette transmission systématique et généralisée des données aboutissant à une surveillance massive et non ciblée.[85] La CNPD se rallie aux observations du Conseil d'État selon lesquelles une transmission non-ciblée des données de l'ensemble des voyageurs qui sont hébergés sur le territoire du Grand-Duché à la Police grand-ducale constitue une ingérence disproportionnée au droit à la protection de la vie privée et au droit à la protection des données à caractère personnel des personnes concernées tels que consacrés par les articles 20 et 31 de la Constitution, l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne et l'article 5 du RGPD.

La transmission de toutes les fiches d'hébergement à la Police grand-ducale

[83] Voir points 9 et s. du présent avis.
[84] Article 5 de la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement.
[85] Avis du Conseil d'État du 12 décembre 2023, doc. parl. n° 8253/02 p. 4.

et la création d'une banque de données, prévue par le nouvel article 43sexies de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, aboutit dès lors à une surveillance disproportionnée des personnes concernées. La jurisprudence européenne considère la conservation généralisée et indifférenciée des données relatives à la localisation des personnes comme incompatible avec les articles 7 et 8 ainsi qu'avec l'article 52.1 de la Charte des droits fondamentaux de l'Union européenne.[86] À cet égard, la Commission nationale tient à rappeler que, conformément à la jurisprudence constante de la Cour de justice de l'Union européenne (ci-après la « CJUE »), les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire.[87] Selon la CJUE, même un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure.

32. La Commission nationale constate que la transmission systématique et généralisée des fiches d'hébergement, effectuées en vertu de la loi actuellement en vigueur, à savoir la loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement, risque d'être contraire à l'article 5 du RGPD, aux articles 7 et 8 ainsi qu'à l'article 52.1 de la Charte des droits fondamentaux de l'Union européenne et aux articles 20 et 31 de la Constitution pour les mêmes motifs qu'énoncés dans le paragraphe 32 du présent avis.

33. Ainsi, la Commission nationale se joint à l'avis du Conseil d'État et invite les auteurs du projet de loi à reformuler les dispositions en se référant aux modèles des législations de nos pays voisins qui demandent aux exploitants de conserver les fiches d'hébergement pendant une durée déterminée et de les mettre uniquement à la disposition de la Police sur demande de celle-ci.

34. Par ailleurs, la Commission nationale note que le projet de loi sous examen prévoit dans son article 10 que le SRE peut demander à la Police grand-ducale la communication des informations et données à caractère personnel qui lui ont été transmises sur base des fiches d'hébergement et qui sont conservées dans sa banque de données. L'accès du SRE est autorisé uniquement si sa demande est fondée sur l'un des motifs énumérés dans la loi à savoir *« pour un ou plusieurs faits qui ont trait à des activités de terrorisme, d'espionnage, de prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes, ou de cyber-menace dans la mesure où celle-ci est liée aux activités précitées »*. La Commission nationale estime qu'il s'agit d'un accès indirect du SRE aux données transmises à la Police grand-ducale et renvoie aux développements sous les points 32 et suivants du présent avis.

XVI. La transmission des données au STATEC

35. Dans un but d'élaborer des données statistiques fiables afin de recenser et

[86] CJUE, arrêt du 21 décembre 2016, *Tele2 Sverige et Watson e.a.*, C-203/15 et C-698/15, EU:C:2016:970, points 50 et s.
[87] CJUE, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 130.

ANNEXES

d'étudier l'évolution des flux touristiques et/ou d'étudier la compétitivité économique de la branche touristique, l'exploitant est obligé de transmettre au STATEC, pour chaque voyageur et chaque séjour, les informations énumérées à l'annexe II du projet de loi sous examen. Comme susmentionné, l'article 9 du règlement (UE) N°692/2011 du Parlement européen et du Conseil du 6 juillet 2011 concernant les statistiques sur le tourisme et abrogeant la directive 95/57/CE du Conseil oblige les États membres de fournir à l'office statistique de la Commission européenne (EUROSTAT) différentes statistiques sur la fréquentation des établissements d'hébergement sur leur territoire.

36. Du commentaire de l'article 6 du projet de loi sous examen il ressort que *« (...) dans la mesure où le STATEC ne se voit transmettre aucune donnée à caractère personnel, le traitement des informations reçues n'est pas soumis à la législation sur la protection des données. »* Les auteurs du projet de loi considèrent que les données transmises au STATEC constituent des données anonymisées dont le traitement n'est pas soumis au régime du RGPD. La CNPD se doit d'émettre des réserves quant à ce raisonnement. En effet, le considérant (26) du RGPD précise qu'il 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. Or, la Commission nationale estime qu'en l'espèce, une combinaison du code postal et de l'année de naissance, données qui sont transmises au STATEC, pourrait permettre l'identification indirecte d'une personne dans des cas particuliers.

37. En vertu du principe de minimisation, prévu par l'article 5.1.c) du RGPD, les données à caractère personnel doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Selon le règlement (UE) N°692/2011 susmentionné, uniquement le pays ou la zone géographique de résidence du visiteur doivent être transmis à la Commission européenne (EUROSTAT).[88] En effet, ledit règlement ne fait pas mention du code postal, qui constitue une donnée beaucoup plus précise que la simple indication du pays ou de la zone géographique. En outre, la CNPD comprend que le règlement susmentionné prévoit que des ventilations sociodémographiques doivent être transmises à la Commission européenne (EUROSTAT), y compris des groupes d'âge.[89]

[88] Selon la section 3 de l'annexe I du règlement (UE) N°692/2011 : *« Les catégories à utiliser pour le pays ou la zone géographique de résidence des clients séjournant dans des établissements d'hébergement touristique sont les suivantes: Union européenne (Union), à déclarer séparément: chaque État membre, Association européenne de libre-échange (AELE) à déclarer séparément: Islande, Norvège et Suisse (y compris le Liechtenstein), autres pays européens (hors Union ou AELE; Russie, Turquie et Ukraine, non inclus), Russie, Turquie, Ukraine, Afrique; à déclarer séparément: Afrique du Sud, Amérique du Nord; à déclarer séparément: États-Unis d'Amérique et Canada, Amérique latine et Amérique centrale; à déclarer séparément: Brésil, Asie; à déclarer séparément: République populaire de Chine, Japon et République de Corée, Australie, Océanie et autres territoires; à déclarer séparément: Australie ».*

[89] Selon la section 1 de l'annexe II du règlement (UE) N°692/2011 : *« Groupe d'âge : moins de 15 ans [facultatif], 15-24, 25-34, 35-44, 45-54, 55-64 ans, 65 ans ou plus, avec des sous-totaux pour les groupes d'âge 25-44 et 45-64 ans. »*

6

Dès lors, la Commission nationale est d'avis qu'il serait opportun de diminuer la granularité des données transmises au STATEC, c'est-à-dire de rendre les informations transmises au STATEC plus générales, afin d'exclure tout risque de réidentification des personnes concernées. À cet égard, la Commission nationale propose de substituer le code postal par le pays ou la zone géographique et de substituer l'année de naissance par des groupes d'âge.

Ainsi adopté à Belvaux
en date du 29 mars 2024.
La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

ANNEXES

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

Délibération n°21/AV9/2024
du 26 avril 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Par courrier en date du 3 octobre 2023, Monsieur le Ministre de l'Énergie et de l'Aménagement du territoire a invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif à la plateforme informatique de données énergétiques, approuvé par le Conseil de gouvernement dans sa séance du 29 septembre 2023 (ci-après le « projet de règlement grand-ducal »).

3. Le projet de règlement grand-ducal entend préciser certaines mesures d'exécution relatives à la plateforme informatique de données énergétiques prévue à l'article 27ter de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité. Les dispositions dudit article avaient d'ores et déjà été commentées par la CNPD dans son avis du 1er juillet 2022 relatif au projet de loi n°7876[90].

4. Elle se prononcera, dès lors, sur les dispositions du projet de règlement grand-ducal ayant un impact en matière de protection de données à caractère personnel.

I. Sur les différents acteurs de la plateforme

5. Les dispositions de l'article 3 du projet de règlement grand-ducal entendent préciser les responsabilités des différents acteurs de la plateforme d'un point de vue du RGPD.

L'article 3.1 du projet de règlement grand-ducal dispose, en effet, que

[90] Délibération n°27/AV11/2022 du 1er juillet 2022 de la Commission nationale de la protection des données, document parlementaire n°7876/04.

« [c]onformément à l'article 27ter, paragraphe 1er, alinéa 1er, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité, le responsable de la plateforme assure le rôle de responsable de traitement au sens du [RGPD] pour l'ensemble des traitements des données énergétiques opérés sur ou par la plateforme. Quant aux données énergétiques visées à l'article 2, paragraphes 1er, point 2°, 2, point 2°, et 4, point 2°, les entreprises d'électricité et de gaz naturel sont des tiers au sens du [RGPD] qui sont responsables de la collecte de ces données auprès des personnes concernées et pour leur importation dans la plateforme. Le responsable de la plateforme est responsable des traitements des données importées au moyen des interfaces visées à l'article 2, paragraphes 1er, point 1°, lettre b), et 4, point 1°, lettre a). Quant aux traitements des données à caractère personnel visés à l'article 2, paragraphe 2, point 1°, lettre a), point ii., les entreprises d'électricité et de gaz naturel y visées sont considérées comme sous-traitants du responsable de la plateforme au sens RGPD ».

6. Il convient de saluer les efforts des auteurs du projet de règlement grand-ducal pour de telles précisions alors que la Commission nationale avait dans son avis du 1er juillet 2022 relatif au projet de loi n°7876 soulevé que *« tant les dispositions légales prévues par le projet de loi que les explications fournies par les auteurs du projet de loi ne permettent pas de déterminer clairement les rôles respectifs du gestionnaire de réseau de transport et des entreprises d'électricité ou de gaz d'un point de vue de la protection des données »*[91].

1) <u>Remarques liminaires</u>

7. Cependant, il y a lieu de relever que l'article 27*ter* de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité précise d'ores et déjà que le gestionnaire de réseau de transport est le responsable du traitement pour les traitements de données à caractère personnel effectués sur la plateforme. Or, le Conseil d'État rappelle que *« les dispositions qui n'ont d'autre objet que de rappeler une disposition hiérarchiquement supérieure, soit en la reproduisant, soit en la paraphrasant, n'ont pas leur place dans les lois et règlements »*[92].

8. En outre, l'article 3.2 du texte sous avis dispose que *« [l]e responsable du traitement procède à une analyse d'impact relative à la protection des données conformément à l'article 35 du RGPD »*. La Commission nationale se demande si de telles dispositions ne sont pas superfétatoires alors que le responsable du traitement doit, en tout état de cause, respecter les obligations qui lui incombent en vertu du RGPD. Parmi celles-ci figure notamment la conduite d'une analyse d'impact conformément à l'article 35 du RGPD lorsque le responsable du traitement identifie des traitements susceptibles *« d'engendrer un risque élevé pour les droits et libertés des personnes physiques concernées ».*

[91] Délibération n°27/AV11/2022 du 1er juillet 2022 de la Commission nationale de la protection des données, document parlementaire n°7876/04, sous point I, B, page 8.
[92] Avis 60.516 du Conseil d'État du 16 juillet 2021, page 8.

ANNEXES

2) <u>Sur le rôle des différents acteurs de la plateforme</u>

9. Les auteurs du projet de règlement grand-ducal précisent dans leur commentaire des articles que si le gestionnaire de réseau de transport est responsable du traitement *« de toutes les opérations opérées sur et par la plateforme, il n'est, conformément à l'alinéa 2 de la disposition précitée, pas responsable de la collecte des données énergétiques auprès des personnes concernées et par conséquent pas responsable de la qualité de ces données »*[93].

10. Comme relevé par les auteurs du projet de texte sous avis, le gestionnaire de réseau de transport serait le destinataire des données collectées par les entreprises d'électricité et de gaz naturel. Le gestionnaire de réseau de transport traiterait ensuite les données reçues pour effectuer des traitements de données via la plateforme informatique.

Il convient dès lors de distinguer :

- Les traitements effectués par les entreprises d'électricité et de gaz naturel, lors de l'importation de données sur la plateforme. Les entreprises d'électricité et de gaz naturel seraient dans ce contexte à qualifier de responsables de traitement ; et

- Les traitements effectués, avec les données reçues, par le gestionnaire de réseau de transport sur la plateforme informatique, qui serait pour de tels traitements à qualifier de responsable du traitement.

11. Par conséquent, dans le cadre de leurs traitements de données respectifs, tant le gestionnaire de réseau de transport que les entreprises d'électricité et de gaz naturel sont tenus de respecter les principes et obligations qui leur incombent en vertu du RGPD. En tant que responsables de traitement, ils doivent notamment respecter les principes visés à l'article 5 du RGPD, dont le principe d'exactitude. En vertu de ce principe, les données personnelles doivent être exactes, et si nécessaire, tenues à jour.

12. La CNPD se permet dès lors de rappeler ses observations formulées dans son avis relatif au projet de loi n°7876, en ce qu'elle avait relevé que *« les dispositions sous avis ne devraient pas décharger le ou les responsables du traitement des obligations qui leur incombent en vertu du RGPD. Ainsi, si le gestionnaire de réseau de transport devait être le responsable du traitement alors les dispositions de l'article 27ter.1. du projet de loi ne devraient pas exclure sa responsabilité quant à la « véracité et l'exactitude des données » qui seraient utilisées via la plateforme »*[94].

En outre, elle avait également rappelé que *« la détermination du responsable du traitement est primordiale alors que c'est sur ce dernier que pèse le respect de l'ensemble des principes énoncés à l'article 5 du RGPD. L'article 24 du RGPD dispose encore à ce sujet que « le responsable du traitement*

[93] V. projet de loi, commentaire des articles, Ad article 3, pages 11 à 12.
[94] Délibération n°27/AV11/2022 du 1er juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, B, page 9.

met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement »[95].

Par conséquent, les dispositions précitées ne sauraient exonérer le gestionnaire de réseau de transport de ses obligations, en tant que responsable du traitement, dans le cadre des traitements effectués sur la plateforme visée par le texte sous avis.

Par ailleurs, il convient d'attirer l'attention des auteurs du projet de règlement grand-ducal sur l'article 19 du RGPD en vertu duquel *« [l]e responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement effectué conformément à l'article 16, à l'article 17, paragraphe 1, et à l'article 18, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés »*. Ainsi, lors des traitements relatifs à l'importation des données sur la plateforme, les entreprises d'électricité et de gaz naturel, en tant que responsables de traitement, devraient notamment notifier au gestionnaire de réseau de transport, en tant que destinataire, *« toute rectification ou tout effacement de données à caractère personnel ».*

13. L'article 3.1 alinéa 2 du projet de règlement grand-ducal dispose que *« [q]uant aux données énergétiques visées à l'article 2, paragraphes 1er, point 2°, 2, point 2° et 4, point 2°, les entreprises d'électricité et de gaz naturel sont des tiers au sens du [RGPD] qui sont responsables de la collecte de ces données auprès des personnes concernées et pour leur importation dans la plateforme ».*

14. Au sujet de ces dispositions, les auteurs du texte sous avis précisent que les entreprises d'électricité et de gaz naturel collectent les données visées par les dispositions précitées et *« assurent le rôle de responsable de traitement au moment de la collecte auprès des personnes concernées et les importent dans la plateforme au moyen d'interfaces mis en place par le responsable de la plateforme. Ils agissent ainsi comme des « tiers » au sens du [RGPD] précité, et sont responsables de leurs propres traitements »*[96].

En vertu de ces dispositions, la Commission nationale comprend que ces dernières seraient donc à considérer comme des responsables de traitement en ce qui concerne l'importation des données sur la plateforme, comme mentionné au point 10 *supra*.

15. Cependant, les auteurs du projet de règlement grand-ducal indiquent encore que les entreprises d'électricité et de gaz naturel agissent comme des « tiers » au sens du RGPD tout en étant *« responsables de leurs propres traitements »*. Il convient de rappeler que l'article 4 du RGPD définit un

[95] Délibération n°27/AV11/2022 du 1er juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, B, page 9.
[96] V. projet de loi, commentaire des articles, Ad article 3, pages 11 à 12.

ANNEXES

tiers comme *« une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel ».*

Or, l'utilisation du terme « tiers » ne semble pas la qualification appropriée alors qu'il ressort des dispositions sous avis et du commentaire des articles que les entreprises d'électricité et de gaz naturel sont à considérer comme responsables des traitements visés aux articles 2.1.2°, 2.2.2° et 2.4.2°. L'emploi du terme « tiers », combiné avec la notion de responsable du traitement dans la même disposition, est susceptible de créer une confusion dans l'esprit du lecteur quant à la qualification juridique desdites entités.

Il est suggéré de remplacer les dispositions actuelles précitées du projet de règlement grand-ducal par les dispositions suivantes : *« [q]uant aux données énergétiques visées à l'article 2, paragraphes 1er, point 2°, 2, point 2° et 4, point 2°, les entreprises d'électricité et de gaz naturel sont à qualifier de responsable du traitement en ce qui concerne la collecte de ces données auprès des personnes concernées et pour leur importation dans la plateforme ».*

Pour le surplus, la CNPD se permet de renvoyer à l'ensemble de ses développements qu'elle avait formulés à ce sujet concernant le projet de loi N°7876[97].

II. <u>Sur les mesures de sécurité</u>

16. Conformément à l'article 5.1.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) ».*

17. 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.

18. Il y a lieu de rappeler qu'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 l'entité concernée, et à quelles données précises cette personne ou ce service aurait accès.

19. En outre, il est nécessaire de prévoir un système de journalisation des accès. Sur ce point, la CNPD recommande que les

[97] Délibération n°27/AV11/2022 du 1er juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, B.

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.

20. Il convient encore de souligner l'importance d'effectuer proactivement des contrôles en interne. A cet effet, il convient conformément à l'article 32.1.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 ».*

21. En outre, tel que relevé par le Conseil d'État dans son avis relatif au projet de loi n°8089 prévoyant notamment la création d'une plateforme sécurisée permettant le stockage d'actes administratifs, *« le RGPD impose au responsable du traitement de mettre en œuvre et de documenter toutes « les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque », notamment compte tenu de l'état des connaissances sachant que l'évolution permanente des meilleures techniques et pratiques en la matière nécessite des adaptations en continu »*[98]. Selon le Conseil d'État, cette exigence devrait s'imposer au responsable du traitement qui devrait mettre en œuvre des mesures au-delà des minima prévus dans un règlement grand-ducal[99].

22. Par ailleurs, la CNPD estime primordial, en ce qui concerne l'accès et la gestion de la plateforme informatique de données énergétiques, 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.

23. Elle se félicite que de telles mesures soient prévues à l'article 2 et soient également précisées et détaillées aux paragraphes 2 et 3 de l'article 4 du projet de règlement grand-ducal. Toutefois, certaines des dispositions appellent les remarques suivantes de la CNPD.

1) Ad article 2

24. L'article 2.2.1°.a) du projet de règlement grand-ducal prévoit notamment les modalités des moyens d'identification aux fins d'attribution d'un identifiant unique pour accéder à la plateforme sous avis. Les moyens d'identification consistent en la vérification de l'identité de l'utilisateur de la plateforme :

- *« à distance par une vérification digitale » ;* ou
- *« aux guichets physiques des entreprises d'électricité et de gaz naturel par le biais d'une vérification de l'identité ».*

25. Quant à la vérification de l'identité de l'utilisateur de la plateforme par les moyens susvisés, il convient de préciser que les dispositions des articles 24[100] et 32 du RGPD seront à respecter, en sus de

[98] Avis 61.218 du Conseil d'État du 12 mars 2024, page 9.
[99] Avis 61.218 du Conseil d'État du 12 mars 2024, page 9.
[100] Voir point 30 paragraphes 3 et 4 du présent avis.

ANNEXES

l'ensemble des principes énoncés à l'article 5 du RGPD[101].

26. En ce qui concerne plus particulièrement la vérification de l'identité de l'utilisateur *« à distance par une vérification digitale », les auteurs du projet de règlement grand-ducal précisent à ce sujet qu' « elle se fait par exemple par l'accès à une application bancaire ou à la plateforme myguichet.lu ».* Il y a lieu de regretter que les modalités pratiques de tels accès ne soient pas plus détaillées dans le commentaire des articles, de sorte que la CNPD ne peut pas réellement analyser quelles seraient les éventuelles questions qui se poseraient en termes de protection des données.

Par ailleurs, en l'absence de précisions quant à l'emploi du terme « digital », la Commission nationale tient à attirer l'attention des auteurs du projet de règlement grand-ducal sur les conséquences de l'éventuel recours à la reconnaissance faciale. Si tel devait être le cas, elle se permet de souligner qu'un tel traitement de données serait à qualifier de traitement de données biométriques. Les dispositions de l'article 9 du RGPD devraient donc être respectées. Elle rappelle que de tels traitements sont en principe interdits à moins que l'une des conditions de l'article 9.2 du RGPD soit remplie et que *« les principes généraux et les autres règles du [RGPD], en particulier en ce concerne les conditions de licéité du traitement »*[102] doivent être respectés.

Notons par ailleurs que le législateur luxembourgeois n'a pas prévu de dispositions nationales spécifiques concernant les données biométriques sur base de l'article 9.4 du RGPD.

2) Ad article 4.2

27. Ainsi, s'il y a lieu de féliciter les auteurs du texte sous avis de prévoir *« un stockage encrypté et isolé sur la plateforme »* des données de comptage visées à l'article 27*ter*.3.b), de la loi modifiée

[101] L'article 5 du RGPD dispose que « 1. Les données à caractère personnel doivent être :
a. traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;
b. collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;
c. adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
d. 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 (exactitude) ;
e. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;
f. 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) ».

[101] V. considérant 51 du RGPD.

du 1er août 2007 relative à l'organisation du marché de l'électricité, dont des données issues des compteurs intelligents, ne faudrait-il pas également prévoir un tel encryptage de données lors de leur importation sur la plateforme par les entreprises d'électricité et de gaz naturel ? En effet, la CNPD avait fait part de ses vives préoccupations dans son avis du 1er juillet 2022 en ce qui concerne l'utilisation de telles données pour des finalités différentes de celles pour lesquelles elles auraient été collectées[103].

28. En outre, concernant la politique de gestion des accès, l'article 4.2.1° du projet de règlement grand-ducal dispose que *« [c]haque utilisateur de la plateforme a accès à ce journal afin de pouvoir retracer les accès et traitements en lien avec les données les concernant ».*

Il convient de préciser que l'accès à ce journal, qui concerne la traçabilité des accès aux traitements de données effectués via la plateforme, devrait en premier lieu pouvoir être effectué par le responsable du traitement de la plateforme afin de pouvoir détecter et, dans la mesure du possible, prévenir que la confidentialité, l'intégralité ou la disponibilité des données traitées via la plateforme ne soient compromises. L'accès à ce journal permet ainsi au responsable du traitement de respecter son obligation de sécurité qui lui incombe en vertu des articles 24 et 32 du RGPD.

Toutefois, la Commission nationale se demande quelles seraient les raisons d'un tel accès par les utilisateurs de la plateforme qui sont définis comme *« toute personne disposant d'un accès individualisé sur la plateforme en vertu de l'article 27ter, paragraphe 5 à 7, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité »*[104].

Il y a lieu de regretter que les auteurs du projet de règlement grand-ducal n'aient pas précisé dans le commentaire des articles les justifications d'un tel accès pour chacun des utilisateurs de la plateforme, à savoir les entreprises d'électricité et de gaz naturel[105], les utilisateurs du réseau et des preneurs de raccordement[106] ainsi que le ministre, le régulateur, Commissaire du Gouvernement à l'Energie ou à l'Institut national de la statistique et des études économiques[107]. Des précisions à ce sujet devraient être apportées.

En outre, si la volonté des auteurs du texte sous examen est de prévoir que cet accès permettrait aux utilisateurs du réseau et des preneurs de raccordement de constater tout accès illicite à leurs données, alors une telle volonté devrait être reflétée dans le projet de règlement grand-ducal. Si cela devait être le cas, la CNPD pourrait accueillir favorablement de telles dispositions, qui permettraient auxdites personnes concernées de se prémunir contre d'éventuels traitements illicites de leurs données à caractère personnel.

[103] Délibération n°27/AV11/2022 du 1er juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, C, pages 10 à 13, et point 3, pages 21 à 23.
[104] V. article 1 du projet de règlement grand-ducal.
[105] V. article 27*ter*.5 de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité.
[106] V. article 27*ter*.6 de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité.
[107] V. article 27*ter*.7 de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité.

ANNEXES

Enfin, compte tenu de la multiplicité des utilisateurs de la plateforme, le responsable du traitement devrait veiller à éviter que des personnes accèdent à des données qui ne les concernent pas et/ou que des utilisateurs accèdent à des données pour lesquelles ces derniers ne devraient pas avoir accès.

3) Ad article 4.3

29. Enfin, l'article 4.3 du projet de règlement grand-ducal dispose que les entreprises d'électricité et de gaz naturel *« mettent en œuvre les mesures techniques et organisationnelles de sécurité appropriées afin de garantir un niveau de sécurité adapté aux risques liés à leurs activités ».*

Il convient de rappeler que les obligations visées aux articles 24 et 32 du RGPD leur incombent en tant que responsable du traitement pour leurs propres traitements de données.

30. De même lorsque celles-ci agissent en tant que sous-traitants du gestionnaire de réseau de transport, alors elles doivent également veiller au respect des mesures de sécurité techniques et organisationnelles conformément aux articles 32.1 et 28.3.c) du RGPD.

Sur ce point, il convient de préciser que *« [t]out traitement de données à caractère personnel effectué par un sous-traitant doit être régi par un contrat ou un autre acte juridique établi par écrit (...). L'accord de traitement ne devrait toutefois pas simplement reproduire les dispositions du RGPD ; il devrait inclure des informations plus spécifiques et concrètes sur la manière dont les conditions seront remplies et sur le niveau de sécurité requis pour le traitement de données à caractère personnel qui fait l'objet dudit accord »*[108].

Il y a lieu de souligner également que *« le responsable du traitement doit toujours stipuler certains éléments dans l'accord de sous-traitance, tels que, en ce qui concerne l'exigence de sécurité, l'instruction de prendre toutes les mesures requises conformément à l'article 32 du RGPD. L'accord doit également indiquer que le sous-traitant doit aider le responsable du traitement à garantir le respect de l'article 32, par exemple. En tout état de cause, le responsable du traitement reste responsable de la mise en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que le traitement est effectué conformément au règlement (article 24) et être en mesure de le démontrer »*[109].

Enfin, le contrat relatif aux activités de traitement *« doit inclure ou mentionner des informations relatives aux mesures de sécurité à adopter, l'obligation faite au sous-traitant d'obtenir le consentement du responsable du traitement avant d'apporter des modifications et le réexamen régulier des mesures de sécurité afin de s'assurer*

[108] LV. Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 du 7 juillet 2021 sur les notions de responsable du traitement et de sous-traitant, page 4, disponibles sous https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

[109] V. Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 du 7 juillet 2021 sur les notions de responsable du traitement et de sous-traitant, para. 41, page 18, disponibles sous https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

de leur adéquation au regard des risques, lesquels peuvent évoluer au fil du temps. Le degré de détail des informations relatives aux mesures de sécurité à inclure dans le contrat doit permettre au responsable du traitement d'apprécier le caractère approprié des mesures conformément à l'article 32, paragraphe 1, du RGPD. En outre, la description est également nécessaire pour permettre au responsable du traitement de se conformer à son obligation de rendre des comptes en vertu de l'article 5, paragraphe 2, et de l'article 24 du RGPD en ce qui concerne les mesures de sécurité imposées au sous-traitant »[110].

III. <u>Remarques finales</u>

31. La Commission nationale se permet de réitérer ses observations en ce qui concerne ses interrogations *« quant aux motivations qui justifieraient qu'une entreprise privée gèrerait une telle plateforme dans l'intérêt public, plutôt que le ministre ayant l'énergie dans ses attributions ou encore l'Institut Luxembourgeois de Régulation (ci-après « l'ILR ») ? »* et renvoie à ses développements formulés dans son avis précité[111].

Ainsi adopté à Belvaux
en date du 26 avril 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[110] V. Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 du 7 juillet 2021 sur les notions de responsable du traitement et de sous-traitant, para. 126, page 42, disponibles sous https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf.

[111] Délibération n°27/AV11/2022 du 1er juillet 2022 de la Commission nationale pour la protection des données, document parlementaire n°7876/04, sous point I, pages 2 à 3.

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8335 relative à la sécurité, la sûreté, l'ordre et la vidéosurveillance dans les transports publics et modifiant la loi du 5 février 2021 sur les transports publics

Délibération n°25/AV10/2024
du 2 mai 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*
2. N'ayant pas été directement saisie par le Ministère de la Mobilité et des Travaux publics, la Commission nationale souhaite néanmoins se prononcer quant au projet de loi n°8335 relative à la sécurité, la sûreté, l'ordre et la vidéosurveillance dans les transports publics et modifiant la loi du 5 février 2021 sur les transports publics (ci-après le « projet de loi »).

3. D'après l'exposé des motifs, une *« augmentation de comportements inconvenants et d'agressions dans les transports publics, envers le personnel de conduite dont particulièrement les chauffeurs d'autobus et le personnel d'accompagnement des trains, tout comme envers le matériel » a été constatée, tandis que les « exploitants déplorent, à juste titre et depuis plusieurs années, que les textes législatifs et réglementaires et les mesures actuellement en place ne sont pas suffisants. »*

Le présent projet de loi vise dès lors à mettre *« en place un meilleur dispositif pour déterminer des règles d'utilisation des transports publics, et pour permettre la constatation et la sanction d'infractions, notamment à l'encontre des comportements qui entravent le bon déroulement des transports publics voire en compromettent l'exécution en toute sécurité. »*

4. La CNPD tient à souligner dès le départ que l'analyse des règles d'utilisation et de comportement par les utilisateurs dans les moyens de transports publics, c'est-à-dire dans tout autobus, tramway ou train

exécutant un service de transports publics,[112] et dans les infrastructures de transports publics comprenant les gares ferroviaires et routières, parkings-relais P+R et arrêts desservis par les services de transports publics[113], tout comme le principe même de l'élargissement des compétences des agents de service des transports publics ne tombent pas dans son champ de compétence.». En revanche, les traitements de données à caractère personnel que lesdits agents sont, le cas échéant, amenés à mettre en œuvre dans ce contexte, tout comme les dispositions sur l'installation des caméras de surveillance dans les moyens et infrastructures de transports publics soulèvent des questions ayant trait à la protection des données à caractère personnel.

XVII. Quant aux traitements de données à caractère personnel opérés par les agents de service des transports publics

5. D'après l'article 24 du projet de loi intitulé *« Traitements des données à caractère personnel »*, les agents visés à l'article 12, c'est-à-dire les agents de service et les agents de service agréés, peuvent, dans l'accomplissement de leurs fonctions, collecter le nom, le prénom, la date de naissance ainsi que l'adresse de la personne ayant commis une infraction susceptible d'être punie d'une des mesures ou sanctions des chapitres 5 et 6 du projet de loi.

Il convient de noter dans ce contexte que le projet de loi opère en effet une distinction entre l'« agent de service », c'est-à-dire toute *« personne employée aux fins de prestation des services de transports publics »,* d'une part, et un tel agent qui est « agréé » par le ministre ayant les Transports dans ses attributions (ci-après le « ministre ») conformément à l'article 8 du projet de loi, d'autre part.[114] Par ailleurs, les services de transports publics visent ceux assurés par les trains, bus et tramways tel que définis à l'article 2 et 4 de la loi du 5 février 2021 sur les transports publics.[115]

a. Remarques préliminaires

6. Tout d'abord, la CNPD tient à souligner qu'elle comprend que d'éventuels traitements de données à caractère personnel dans le cadre des constats d'infractions visés à l'article 9 précité du projet de loi peuvent uniquement être mis en œuvre par des agents de service qui sont « agréés ». Elle recommande dès lors aux auteurs du projet de loi d'adapter l'article 24, deuxième alinéa en ce sens.

7. De même, la Commission nationale constate que le paragraphe 1er dudit article 24 du projet de loi se réfère qu'aux *« données à caractère personnel visées par le présent chapitre »,* alors que ce chapitre (le chapitre 6) concerne uniquement la vidéosurveillance et non les traitements de données à caractère personnel opérés dans

[112] D'après l'article 2 point 9° du projet de loi.
[113] Voir article 1er du projet de loi.
[114] Voir définitions de « agent de service » et « agent de service agréé » aux points 5° et 6° de l'article 2 du projet de loi.
[115] Voir article 1er du projet de loi et son commentaire des articles.

ANNEXES

le cadre des nouvelles missions des agents de service agréés.

Par ailleurs, la référence aux mesures ou sanctions du chapitre 5 et 6 dans le même article 24 du projet de loi semble erronée. En effet, le chapitre 5 vise uniquement les infractions et sanctions pénales recherchées et constatées par la Police grand-ducale et l'Administration des Douanes et Accises (ci-après « ADA ») et non pas par les agents de service prémentionnés, tandis que le chapitre 6 contient, comme susmentionné, les dispositions concernant la vidéosurveillance, mais sans prévoir une quelconque sanction.

8. Au vu de ce qui précède, la CNPD recommande aux auteurs du projet de loi de supprimer l'article en cause et d'insérer les dispositions en matière de traitements de données à caractère personnel au chapitre 3 du projet de loi sur les sanctions administratives, d'une part, ainsi qu'au chapitre 5 en ce qui concerne les infractions pénales, d'autre part. Alternativement, l'article 24 du projet de loi devrait être modifié en tenant compte des remarques précédentes et en distinguant entre les traitements de données opérés par les agents de transports agrées et celles mis en œuvre par la Police grand-ducale et l'ADA.

b. Quant au responsable du traitement

9. La CNPD tient à rappeler que conformément à l'article 4.7) du RGPD, le responsable du traitement est *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; 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. »*

10. En ce qui concerne plus précisément les notions de responsable du traitement et de sous-traitant, il ressort des lignes directrices du Comité européen de la protection des données (ci-après : « CEPD ») sur ce sujet que *« [l]orsque le responsable du traitement est spécifiquement identifié par la loi, cette désignation est déterminante pour définir qui agit en tant que responsable du traitement. Cela présuppose que le législateur a désigné comme responsable du traitement l'entité qui est véritablement en mesure d'exercer le contrôle. »*[116]

11. Il est encore à noter que la notion de responsable du traitement, voire de responsabilité conjointe, sont des notions fonctionnelles en ce qu'elles visent à répartir les responsabilités en fonction des rôles réels joués par les parties prenantes. Ainsi, elles reposent sur une analyse factuelle plutôt que formelle.[117]

12. En l'espèce, de multiples acteurs sont impliqués qui, le cas échéant, peuvent procéder à différents traitements de données à caractère personnel :

[116] CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.0, adoptées le 7 juillet 2021, point 23.
[117] Page 3 et points 21 et 52 desdites lignes directrices.

- Les agents de service agréés procèdent à des constats d'infractions conformément à l'article 9 du projet de loi.

- Une copie desdits constats est envoyée au ministre qui prononce, le cas échéant, une amende administrative sur base de l'article 10.1 du projet de loi qui prévoit que l'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement de ces amendes.

- Le ministre peut aussi émettre des décisions d'interdiction d'accès et de séjour dans les moyens et infrastructures de transports publics qui sont notifiées à l'usager. Une information est faite dans ce cas à la Police grand-ducale et à l'ADA.[118]

- Des avertissements taxés peuvent être émis par la Police grand-ducale et l'ADA conformément aux articles 15 à 20 du projet de loi.

13. De manière générale, la Commission nationale est d'avis qu'il pourrait ressortir de l'économie générale du projet de loi que le ministre, la Police grand-ducale, ainsi que l'ADA sont à considérer chacun pour soi comme responsable des traitements de données à caractère personnel qu'ils mettent en œuvre afin d'assumer les missions que le projet de loi leur impose.

14. Elle tient à souligner dans ce contexte que les traitements de données à caractère personnel mis en œuvre, le cas échéant, par la Police grand-ducale, et même par l'ADA dans le cadre des infractions pénales qu'elles peuvent sanctionner, tombent dans le champ d'application de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

15. La CNPD estime cependant qu'il ne ressort ni du texte du projet de loi, ni du commentaire des articles qui est à qualifier de responsable des traitements de données à caractère personnel mis en œuvre par les agents de service agréés lorsqu'ils procèdent à des constats d'infractions sur base de l'article 9 du projet de loi. Est-ce qu'il s'agit de chaque employeur[119] desdits agents qui offrent des prestations de service de transports publics, tant du secteur public que du secteur privé ou, en revanche, du ministre qui assumerait dès lors la responsabilité générale pour les traitements de données dans le cadre des constatations d'infractions qui peuvent, le cas échéant, faire l'objet d'une des sanctions administratives visées à l'article 7.3 du projet de loi ?

Elle recommande donc aux auteurs du projet de loi de préciser dans le corps du texte qui est à qualifier de responsable des différents traitements de données à caractère personnel mis en œuvre.

c. Quant au contrôle d'identité

[118] Voir l'article 14 du projet de loi.

[119] Voir dans ce contexte les lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, point 19 : *« En principe, tout traitement de données à caractère personnel effectué par des employés dans le cadre des activités d'une organisation peut être réputé avoir lieu sous le contrôle de celle-ci. »*

ANNEXES

16. D'après l'article 7.4 du projet de loi, les agents de service agréés, les membres de la Police grand-ducale relevant du cadre policier et les agents de l'ADA sont autorisés, en cas de constatations des infractions donnant lieu à une sanction administrative, à contrôler l'identité des usagers et à se faire exhiber à ces fins une pièce d'identité.

Le commentaire des articles précise uniquement que l'*« identité est nécessaire pour déclencher les procédures prévues par les articles afférents ».*

17. La CNPD s'étonne que le législateur ait choisi d'étendre les prérogatives des officiers et agents de police judiciaire dans le cadre des vérifications d'identité prévues à l'article 45 du Code de procédure pénale à d'autres acteurs, d'autant plus que ces derniers peuvent, le cas échant, être des employés engagés par des sociétés privées.[120]

18. Par ailleurs, même si l'article 7.4 du projet de loi prévoit que le *« refus d'exhiber une pièce d'identité est puni d'une amende de 25 à 250 euros »,* la CNPD se demande de quels moyens coercitifs les agents de service agréés peuvent se prévaloir en cas de refus ou d'impossibilité d'un usager de produire une pièce d'identité. En effet, la rétention de la personne se trouvant dans une telle situation ou sa conduite au poste de police aux fins de vérifications de son identité constitue un pouvoir accordé par le Code de procédure pénale uniquement à la Police grand-ducale.[121]

d. Quant au constat des infractions et à l'injonction de quitter les transports publics

19. D'après les articles 9.1 et 9.2 du projet de loi, l'agent de service agréé peut constater *« par écrit ou par moyen électronique »* les infractions qui font l'objet de sanctions administratives dont il est le témoin direct, d'une part, et que ce *« constat écrit ou électronique fait foi des faits y constatés, jusqu'à preuve du contraire »*, d'autre part.

La CNPD estime qu'il n'est pas opportun de faire une différence entre un constat « écrit » et un constat « électronique », alors qu'un constat électronique se manifeste aussi sous forme écrit. Elle suppose que les auteurs du projet de loi ont envisagé de différencier entre un constat rédigé de manière manuelle et un constat sous forme électronique et elle leur recommande d'adapter le texte de l'article 9 du projet de loi en ce sens.

20. Par ailleurs, conformément aux articles 9.1 et 9.4 du projet de loi, une copie du constat est envoyée au ministre, tandis que l'original est remis au contrevenant. Sur base des dispositions précitées, la CNPD suppose dès lors qu'aucune copie dudit constat ne sera pas gardée par l'agent de service agréé. Dans le cas contraire et sans justifications supplémentaires dans le commentaire des articles, la Commission nationale ne peut pas se prononcer sur la nécessité de conserver une copie des constats par les agents en cause. En effet,

[120] Comme par exemple la société Luxtram S.A. ou encore des sociétés privées exploitant des lignes de bus de transport public au Luxembourg comme Voyages Emile Weber sàrl, S.L.A. S.A. ou Demy Schandeler S.à r.l.

[121] Voir article 45.2 du Code de procédure pénale : *« Si l'intéressé refuse ou se trouve dans l'impossibilité de prouver son identité, il peut être retenu sur place ou conduit au poste de police aux fins de vérifications de son identité. »*

conformément à l'article 5.1.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). »*

21. Elle constate de même que l'article 9.5 du projet de loi prévoit que la personne ayant commis une infraction a *« accès au dossier et est mise à même de présenter ses observations écrites dans un délai de deux semaines à partir de la remise du constat précité »*. Néanmoins, il ne ressort ni du texte du projet de loi, ni de son commentaire des articles auprès de qui le droit d'accès est à exercer et à qui les observations sont à adresser : à l'agent de service agréé ayant rédigé le constat ou directement au ministre ?

22. En ce qui concerne les injonctions de quitter les transports publics conformément à l'article 13 du projet de loi, les agents de service et agents de service agréés peuvent enjoindre *« aux usagers qui refusent d'obtempérer à un rappel à l'ordre, de quitter le moyen de transports publics ou de s'éloigner des lieux »*, tandis qu'uniquement les membres de la Police grand-ducale et de l'ADA sont autorisés à les contraindre par la force.

Cette interdiction prend fin après deux heures, le commentaire des articles précisant que la *« loi de 2009 [...] prévoyait encore l'établissement de rapports lors d'une injonction de quitter les lieux ou encore une information concernant une expulsion. Considérant dans la pratique que ceci n'avait pas lieu puisqu'il n'y avait pas de plus-value, les auteurs ne prévoient plus de telle disposition dans le nouveau texte. »*

23. La Commission nationale s'interroge néanmoins comment le respect de cette injonction de quitter les transports publics pendant deux heures, voire comment une potentielle violation de ladite injonction pourrait être prouvée sans trace écrite. Elle se demande dès lors si l'agent en cause ne se noterait pas l'identité de l'usager et les heures de l'interdiction, procédant de telle manière à un traitement de données à caractère personnel. Dans ce cas, elle estime que des précisions seraient à insérer dans le texte du projet de loi.

XVIII. Quant à la vidéosurveillance

24. L'article 21.1 du projet de loi prévoit la mise en place d'une vidéosurveillance *« par installation de caméras à bord et à l'extérieur des moyens de transports publics, ainsi que dans les infrastructures de transports publics [...]. »* Comme mentionné au point 4 du présent avis, par « moyens de transports publics » sont visés les autobus, tramways et trains exécutant un service de transports publics, tandis que les « infrastructures de transports publics » comprennent les gares ferroviaires et routières, les parkings-relais P+R et les arrêts desservis par les services de transports publics.[122]

D'après le commentaire des articles, cet article vise à créer *« une base légale pour*

[122] Voir article 1er et article 2 point 9° du projet de loi. Voir aussi les définitions de « gare ferroviaire », « gare routière » et « point d'arrêt » prévues à l'article 2, points 1°, 2° et 4° du projet de loi.

ANNEXES

l'installation de caméras de surveillance dans et sur les moyens de transports publics de personnes et dans les infrastructures de transports publics et en définit les finalités. »

25. Le captage et l'enregistrement par de tels caméras de surveillance d'images de personnes identifiables ou de véhicules dont la plaque minéralogique apparaît lisiblement sur les images constituent un traitement de données à caractère personnel au sens du RGPD.

De manière générale, la CNPD se félicite dès lors que le projet de loi entend conférer une base légale aux traitements de données effectués dans le cadre de la mise en place des caméras précitées. Elle note que lesdites caméras poursuivent différentes finalités énumérées à l'article 21.1 du projet de loi, comme par exemple « *sécuriser les accès aux moyens de transports publics* », « *assurer la sécurité des personnes et protéger les bien* », ou encore « *permettre aux autorités compétentes et aux opérateurs de prendre les mesures appropriées et nécessaires en cas d'accidents et d'incidents* ». Leur mise en place dans les moyens et infrastructures de transports publics pourrait dès lors correspondre à une mission d'intérêt public conformément à l'article 6.1.e) du RGPD. Néanmoins, différentes conditions sont à respecter dans ce contexte que la CNPD tient à rappeler dans ses remarques préliminaires, avant d'analyser plus en détail le fond des dispositions en la matière contenues au projet de loi.

a. Remarques préliminaires

26. La CNPD estime tout d'abord que l'article 6.1.e) du RGPD, lu en combinaison avec l'article 6.3 du RGPD, prévoit dans ce contexte une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect 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. Dans ce cas de figure, le fondement, c'est-à-dire la mission d'intérêt public en cause, et notamment les finalités des traitements de données doivent ressortir soit du droit de l'Union européenne, soit du droit de l'État membre auquel le responsable du traitement est soumis et ce fondement doit répondre *« à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi. »*

27. Dans un arrêt récent, la Cour de Justice a par exemple estimé que la *« détermination des finalités et des moyens du traitement et, le cas échéant, la désignation de ce responsable par le droit national peuvent être non seulement explicites, mais également implicites. Dans ce dernier cas de figure, il est néanmoins requis que cette détermination découle de manière suffisamment certaine du rôle, de la mission et des attributions dévolus à la personne ou à l'entité concernée. »*[123]

28. En droit interne, il est à noter que l'article 31 de la Constitution révisée, applicable depuis le 1er juillet 2023, dispose que *« [t]oute personne a droit à l'autodétermination informationnelle et*

[123] CJUE, arrêt du 11 janvier 2024, État belge/Autorité de protection des données, C-231/22, EU:C:2024:7, point 30.

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. »

29. Dès lors, en tenant en compte que la protection des données à caractère personnel est une matière réservée à la loi par la Constitution, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc.[124] En effet, d'après la jurisprudence de la Cour constitutionnelle, l'article 45.2 de la Constitution exige que dans ces matières, *« la fixation des objectifs des mesures d'exécution doit être clairement énoncée, de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi »*[125]

30. Ensuite, il faut prendre en compte que les droits fondamentaux ne sont pas des prérogatives absolues puisque la possibilité d'une ingérence ou d'une limitation est prévue tant par l'article 8.2 de la Convention européenne des droits de l'homme, que par l'article 52.1 de la Charte des droits fondamentaux de l'Union européenne, ainsi que par l'article 37 de la Constitution luxembourgeoise révisée qui prévoit que *« [t]oute limitation de l'exercice des libertés publiques doit être prévue par la loi et respecter leur contenu essentiel. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires dans une société démocratique et répondent effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui. »*

31. La Commission nationale estime dès lors que si les traitements de données mis en œuvre par des entités dans le cadre de l'exécution de leurs missions d'intérêt publique constituent une ingérence dans la vie privée des citoyens, ces traitements doivent être spécifiquement encadrés par une loi au sens formel. En effet, une ingérence ou limitation dans l'exercice des libertés publiques peut uniquement 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, respecte le contenu essentiel du droit à la protection des données et réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui. Finalement, l'ingérence doit être nécessaire dans une société démocratique, sous réserve du principe de proportionnalité.[126]

32. Le fait d'effectuer des enregistrements d'images par des caméras de surveillance dans les moyens et infrastructures de

[124] Voir articles 31 et 45 de la Constitution luxembourgeoise.
[125] Cour constitutionnelle, 4 juin 2021, n° 166, Mém. A n°440 du 10 juin 2021 et Cour constitutionnelle, 3 mars 2023, n° 177, Mém. A, n° 127 du 10 mars 2023.
[126] Pour une analyse plus détaillée de ces conditions, voir délibération n°2/2021 du 4 février 2021 de la Commission nationale pour la protection des données, doc. parl. n°7425/09, point I.1.b). Voir aussi arrêt de la CJUE du 7 mars 2024, Endemol Shine Finland Oy, C-740/22, EU:C:2024:216, point 52.

ANNEXES

transports publics, ayant potentiellement des personnes physiques dans leurs champs de vision qui n'ont pas exprimé leur consentement, constitue une telle ingérence importante dans l'exercice du droit à la vie privée et de la protection des données à caractère personnel et doit dès lors respecter les conditions susmentionnées.

b. Quant au responsable du traitement

33. La CNPD se permet tout d'abord de renvoyer aux points 9 à 11 du présent avis sur la notion de responsable du traitement, voire de responsabilité conjointe. Elle tient à ajouter que cette responsabilité *« peut être définie par la loi ou découler d'une analyse des éléments ou circonstances factuels de l'espèce. […] Toutefois, plus fréquemment, plutôt que de désigner directement le responsable du traitement ou de définir les critères applicables à sa désignation, la législation confiera une mission ou imposera à quelqu'un l'obligation de collecter et de traiter certaines données. Dans ces cas, la finalité du traitement est souvent déterminée par la loi. Le responsable du traitement sera normalement celui désigné par la loi en vue de la réalisation de cette finalité, de cette mission de service public. »*[127]

34. Déterminer qui décide d'installer dans quel moyen et sur quelle infrastructure de transports publics des caméras de surveillance est dès lors fondamentale afin de savoir qui doit respecter les droits consacrés aux personnes concernées, ainsi que les obligations imposées par le RGPD.

35. Néanmoins, la Commission nationale considère qu'il ne ressort ni du texte du projet de loi ou du commentaire des articles, ni même indirectement des éléments ou circonstances factuels en cause qui serait à considérer comme responsable du traitement des données à caractère personnel collectées à travers la mise en place des caméras de surveillance. En d'autres termes, sur base des dispositions du projet de loi, il n'est pas possible de déterminer à quelle entité précise incombe la réalisation des finalités prévues à l'article 24.1 du projet de loi. S'agirait-il des différents opérateurs offrant des services de transports publics[128], permettant, le cas échéant, à des sociétés privées d'installer des caméras sur la voie publique, ou, par contre, du ministre, voire de l'Administration des transports publics ? Une responsabilité conjointe entre les opérateurs précités et le ministre paraît, le cas échéant,envisageable.

36. Au cas où le ministre serait à considérer comme responsable du traitement, la CNPD se demande si ce dernier décide unilatéralement et de sa propre initiative à quels endroits et combien de caméras sont à installer ou si les différents opérateurs ont la possibilité de demander une autorisation d'installation de caméras au ministre. Si un tel système est prévu, il est important d'en définir les modalités dans le texte du projet de loi.

[127] CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.0, adoptées le 7 juillet 2021, points 20 et 24.

[128] Comme la Société Nationale des Chemins de Fer Luxembourgeois (C.F.L.), le syndicat des tramways intercommunaux dans le canton d'Esch (TICE), Luxtram S.A. ou encore d'autres sociétés privées exploitant dans le cadre du Régime général des transports routiers (RGTR) des lignes de bus de transport public au Luxembourg comme Voyages Emile Weber sàrl, S.L.A. S.A. ou Demy Schandeler S.à r.l.

À titre de comparaison, en Belgique la loi modifiée du 21 mars 2007 réglant l'utilisation de caméras de surveillance prévoit en son article 5 que le responsable du traitement qui veut installer des caméras de surveillance fixes dans un lieu ouvert (comme par exemple sur un arrêt de bus ou de tram) ne peut être qu'une autorité publique, d'une part, et que cette autorité doit avoir reçu un avis positif du conseil communal après consultation préalable du chef de corps de la zone de police, d'autre part.

37. La Commission nationale estime dès lors qu'il est primordial de préciser dans le corps du texte du projet de loi qui est à qualifier de responsable, voire de responsable(s) conjoint(s) des traitements mis en œuvre dans le cadre des caméras de surveillance dans et sur les moyens de transports publics, ainsi que dans les infrastructures en cause.

c. Quant aux finalités poursuivies

38. Au titre du respect des principes relatifs au traitement des données à caractère personnel tels qu'ils sont prévus par le RGPD, la CNPD rappelle que les données à caractère personnel doivent être *« collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités [...] (limitation des finalités) » et qu'elles doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données). »*[129]

39. En l'espèce, l'article 21.1 du projet de loi énumère sept différentes finalités poursuivies par la mise en place des caméras à bord et à l'extérieur des moyens et infrastructures de transports publics. Néanmoins, en ce qui concerne plus particulièrement la finalité n°3 consistant à *« permettre la poursuite d'infractions pénales »,* la CNPD se demande quelle est l'interaction entre le projet de loi sous avis et la loi modifiée du 18 juillet 2018 sur la Police grand-ducale. En effet, comme les caméras dans les différentes infrastructures de transports publics, dont notamment celles visant les arrêts desservis par les services de transports publics, tout comme les caméras placées à l'extérieur des moyens de transports publics[130] ont vocation à filmer la voie publique, l'article 43*bis*, paragraphe 1er de la loi précitée est susceptible de s'appliquer. En vertu de cette disposition, la *« Police peut, avec l'autorisation du ministre et si les autres moyens mis en œuvre pour empêcher la commission d'infractions pénales se sont avérés inefficaces, placer sous vidéosurveillance aux fins de la prévention, de la recherche et de la constatation d'infractions pénales les lieux accessibles au public qui présentent un risque particulier de commission d'infractions pénales. »*

40. La CNPD estime donc que la mise en place des caméras de surveillance sur base du projet de loi sous examen à l'extérieur des moyens et dans les infrastructures de transports publics, qui sont de par leur nature accessibles au public, afin de poursuivre d'infractions pénales risque

[129] Voir article 5.1.b) et e) du RGPD.
[130] Voir dans ce contexte les points 41 à 43 du présent avis.

ANNEXES

d'empiéter sur les prérogatives de la Police grand-ducale conformément à l'article précité de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale. En d'autres mots, la poursuite de cette finalité par un responsable du traitement sur base de l'article 21 du projet de loi ne peut pas être considérée comme « légitime » au sens de l'article 5.1.b) du RGPD, alors que la réalisation de cette finalité est une mission réservée par la loi à la Police grand-ducale. Il doit dès lors être évité que le projet de loi sous avis permettrait de contourner les conditions et modalités prévues par l'article 43*bis*, paragraphe 1er de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale afin de placer sous vidéosurveillance aux fins de la prévention, de la recherche et de la constatation d'infractions pénales les lieux accessibles au public.

41. Finalement, en prenant en compte que l'article 21 du projet de loi permettrait la mise en place de caméras « à l'extérieur » des moyens de transports publics, la CNPD suppose que sont visées des caméras mobiles installées sur les bus, trains ou tram, c'est-à-dire de type « dashcams ».

42. En France, la loi du 25 mai 2021 pour une sécurité globale préservant les libertés prévoit la mise en place, à titre expérimental, de telles caméras frontales embarquées sur les matériels roulants exploités par les opérateurs de transport public ferroviaire de voyageurs. Néanmoins, les finalités que de telles caméras peuvent poursuivre sont beaucoup plus limitées. En effet, l'article 61 de la loi précitée prévoit que les *« traitements prévus au présent article ont exclusivement pour finalité d'assurer la prévention et l'analyse des accidents ferroviaires ainsi que la formation des personnels de conduite et de leur hiérarchie. »*

43. Au vu du principe de minimisation des données et de limitation des finalités et en raison du défaut d'explications sur les finalités poursuivies dans le commentaire des articles, la CNPD se demande dès lors si de telles dashcams sont vraiment nécessaires pour atteindre toutes les finalités énumérées à l'article 21.1 du projet de loi oui si, par contre, une distinction s'impose entre les finalités poursuivies par les caméras installées dans les moyens de transports publics, par celles à l'extérieur desdits moyens (c'est-à-dire les dashcams), ainsi que par celles mises en place dans les infrastructures de transports publics.

d. Quant aux champs de vision et au nombre de caméras

44. Sans préjudice de ses commentaires précédents sur la notion de responsable du traitement, voire sur les finalités poursuivies par les traitements mis en œuvre par les caméras qui peuvent être installées dans et à l'extérieur des moyens et infrastructures de transports publics conformément à l'article 27.1 du projet de loi[131], la CNPD se demande si le(s) responsable(s) du traitement ont uniquement la possibilité d'installer de telles caméras ou si, en revanche, la future loi leur imposerait une obligation de les mettre en place.

[131] Voir points 33 à 37 du présent avis sur la problématique concernant la définition du responsable du traitement et points 38 à 43 sur les finalités poursuivies.

45. De même, il ne ressort ni du texte du projet de loi, ni du commentaire des articles, si des caméras seront potentiellement installées sur tous les gares, parkings et arrêts desservis par les services de transports publics ou que sur des points stratégiques qui remplissent certaines conditions (par exemple des lieux particulièrement exposés à des risques d'accidents, de dégâts, d'agressions, de vols ou d'atteintes à la sécurité des personnes ou des biens).[132]

La CNPD tient à souligner dans ce contexte que l'installation de caméras partout sur le réseau des transports publics pourrait conduire à ce que quasi la totalité de la voie publique au Luxembourg serait sous vidéosurveillance, ce qui risque d'être en contradiction avec le principe de proportionnalité et de nécessite, combiné avec le principe de minimisation des données. Elle estime dès lors qu'il est important de fixer dans le corps du texte du projet de loi des critères objectifs encadrant la mise en place des caméras de surveillance afin d'éviter toute collecte disproportionnée de données à caractère personnel, tout en respectant les principes de prévisibilité et de qualité de la loi tels que prévus par le droit de l'Union européenne.

46. Par ailleurs, à l'instar de ce qui est prévu à l'article 43*bis*, paragraphe (5), alinéa 2, de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, la CNPD recommande aux auteurs du projet de loi d'intégrer dans le texte du projet de loi une disposition prévoyant que le *« [l]e recours à des techniques de reconnaissance faciale est exclu ».*

47. Finalement, la CNPD tient à souligner que les employés des différents opérateurs de transports publics ont en principe le droit de ne pas être soumis à une surveillance permanente et continue, surtout à travers les caméras installées à l'intérieur des moyens de transports publics. Afin d'éviter une telle surveillance, le responsable du traitement doit limiter le champ de vision des caméras à la seule surface nécessaire pour atteindre les finalités poursuivies.[133]

e. Quant à l'information des personnes concernées

48. L'article 22.2 du projet de loi prévoit que les personnes concernées sont *« informées de l'existence d'un système de vidéosurveillance par l'apposition de pictogrammes et de panneaux d'affichage à l'entrée des moyens de transports publics, ainsi que sur les arrêts et les quais. »*

49. La CNPD tient à souligner que par « personne concernée » est visée toute personne physique identifiée ou identifiable.[134] En l'espèce, sont dès lors ciblés non seulement les individus utilisant les moyens de transports publics, ainsi que les piétons qui traversent la voie publique, mais, aussi, les propriétaires de véhicules dont la plaque minéralogique est clairement lisible, même si les personnes elles-mêmes

[132] Voir dans ce contexte l'article 43*bis*, deuxième paragraphe de la loi modifiée du 18 juillet 2018 sur la Police grand-ducal qui énumère les lieux présentant un risque particulier de commission d'infractions pénales.
[133] Voir lignes directrices de la CNPD en matière de vidéosurveillance, mise à jour le 05/04/2024, page 10.
[134] Voir définition au point 1) de l'article 4 du RGPD.

ANNEXES

n'apparaissent pas directement dans le champ de vision des caméras.
Cette obligation d'information desdites personnes concernées incombe au responsable du traitement conformément à l'article 13 du RGPD. Le commentaire des articles précise que les personnes concernées sont informées *« par l'apposition d'affiches et d'une notice d'information dans les endroits concernés, ainsi que sur le site internet de l'Administration des transports publics ou autres »*. Alors qu'elle ne peut que soutenir de manière générale l'approche d'informer en deux niveaux afin de faciliter la compréhension des personnes concernées sur les traitements de données effectués lors de l'utilisation d'un système de vidéosurveillance, elle constate que la terminologie utilisée dans le commentaire des articles *(« sur le site internet de l'Administration des transports publics ou **autres** »)* renforce la problématique de la définition du responsable du traitement comme détaillé aux points 33 à 37 du présent avis.

50. En ce qui concerne plus précisément l'information en deux niveaux, une telle approche consiste à communiquer – dans un premier temps – une série d'informations aux personnes concernées, par exemple par des panneaux d'affichage comme mentionné par les auteurs du projet de loi, et puis – dans un second temps – à communiquer via d'autres moyens, tel un site internet, l'ensemble des informations requises au titre de l'article 13 du RGPD. En ce qui concerne le contenu obligatoire du premier et deuxième niveau d'information, la CNPD se permet de renvoyer à ses lignes directrices en matière de vidéosurveillance.[135]

51. Cependant, la Commission se demande comment le responsable du traitement veut matériellement respecter son obligation d'information des individus de l'existence d'éventuelles « dashcams » installées à l'extérieur des moyens de transports publics, alors que les informations doivent leur parvenir « au moment où les données en question sont obtenues » conformément à l'article 13 du RGPD, c'est-à-dire qu'elles *« doivent être placées de telle sorte que la personne concernée puisse facilement reconnaître les circonstances de la surveillance avant de pénétrer dans la zone surveillée (approximativement à hauteur des yeux). »*[136]

52. De même, au cas où les caméras de vidéosurveillance viseraient des salariés du (des) responsable(s) du traitement, la CNPD attire l'attention des responsables du traitement sur les obligations additionnelles, notamment en matière d'information collective, prévues à l'article L. 261-1 du Code du travail.[137]

53. Finalement, la CNPD tient à souligner que par principe, toute personne concernée dispose du droit de s'opposer *« à tout moment, pour des raisons tenant à sa situation particulière, a un traitement des données à caractère personnel la*

[135] Voir lignes directrices de la CNPD en matière de vidéosurveillance, mise à jour le 05/04/2024, pages 6 et 7.
[136] CEPD, Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des dispositifs vidéo, version 2.0, adoptée le 29 janvier 2020, point 113.
[137] Voir aussi l'avis III/2/2024 de la Chambre des salariés du 7 février 2024 relatif au projet de loi sous avis, point 10.

concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions » conformément à l'article 21 du RGPD. Dans ce cas, « le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice. »[138]

54. Néanmoins, des limitations à la portée dudit droit peuvent être prévues par le droit de l'Union européenne ou le droit d'un État membre par voie de mesure législative sur base de l'article 23 du RGPD. Or, ledit article prévoit en son paragraphe 1er que les droits de la personne concernée peuvent être limités lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs énumérés dans ce paragraphe. Par ailleurs, il y a lieu de soulever que lorsqu'une telle restriction aux droits des personnes est prévue par une mesure législative, elle doit contenir des dispositions spécifiques relatives aux informations énumérées au paragraphe 2 de l'article 23 du RGPD.[139]

55. En l'espèce, la CNPD ne voit pas comment les personnes concernées pourraient bénéficier de leur droit de s'opposer au traitement de leurs données à caractère personnel par les caméras installées sur et dans les moyens et infrastructures de transports publics. Elle estime dès lors qu'une telle limitation du droit d'opposition doit être insérée dans le texte du projet de loi et les conditions de l'article 23 susmentionné du RGPD sont à respecter.

f. Quant à la durée de conservation des images

56. Sur base de l'article 23 du projet de loi, les enregistrements comportant des données à caractère personnel sont effacés après six mois, sauf lorsqu'ils sont utilisés dans le cadre d'une procédure judiciaire, administrative ou disciplinaire.

57. La CNPD se demande tout d'abord si un visionnage 24/7 en temps réel des images est prévu pour assurer l'effet préventif dans le cadre de la réalisation des finalités visées à l'article 21.1 points 4° et 6° du projet de loi ou si les enregistrements sont visionnés uniquement a posteriori en cas d'incident.

58. En ce qui concerne ensuite la durée de conservation, l'article 5.1.e) du RGPD oblige le responsable du traitement à ne pas conserver les données à caractère personnel pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

Le commentaire des articles précise dans ce contexte qu'*« [a]u vu des procédures et des*

[138] Voir article 21.1, deuxième phrase du RGPD.

[139] Il s'agit des finalités du traitement ; des catégories de données à caractère personnel; de retendue des limitations introduites ; des garanties destinées à prévenir les abus ou l'accès ou le transfert illicites; la détermination du responsable du traitement; les durées de conservation et les garanties applicables ; les risques pour les droits et libertés des personnes concernées et le droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation.

ANNEXES

différents acteurs impliqués (constat d'une infraction, dépôt d'une plainte, établissement d'un procès-verbal, ordonnance de saisie par le juge d'instruction…) ou encore en cas de plainte tardive de la part de la victime, et en concertation avec le Parquet général, [la durée de conservation] est fixée à 6 mois afin de permettre la poursuite des infractions par les autorités publique. »

59. La CNPD considère de manière générale que pour les traitements de données mis en œuvre par un système de vidéosurveillance nécessaire aux fins des intérêts légitimes du responsable du traitement,[140] une durée de conservation de 8 jours semble appropriée, sauf cas exceptionnel justifiant une durée de 30 jours.[141]

60. Dans le cas d'espèce et en raison des arguments mentionnés par les auteurs dans le commentaire des articles, elle comprend néanmoins qu'une durée de conservation de 8 jours ne pourrait pas être suffisante afin de réaliser les finalités visées. Cependant, en analysant d'autres systèmes de vidéosurveillance visant la voie publique et encadrés par un texte légal au niveau national, la CNPD constate que les durées de conservation sont moins longues. À titre d'exemples, l'article 43*ter*, paragraphe 7, de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale prévoit une durée de conservation de 28 jours pour les images enregistrées par les caméras-piétons de la Police grand-ducale, tandis que l'article 43*bis*, paragraphe 1er de la loi précitée encadrant le système VISUPOL définit une durée de stockage de deux mois.

61. En ce qui concerne la réglementation française et belge concernant des caméras visant potentiellement la voie publique, il convient de préciser ce qui suit :

- En Belgique, un arrêté royal du 6 décembre 2018 fixe la liste des lieux qui par leur nature présentent un risque particulier pour la sécurité et pour lesquels les images des caméras de surveillance pourront être conservées trois mois au lieu de la durée de conservation générale d'un mois prévu par la loi modifiée du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance. En vertu de l'article 3, deuxième point dudit arrêté le délai maximum de conservation des images dans *« les gares et les véhicules de transport public des sociétés publiques de transport en commun »* est en effet prolongé à trois mois.[142] Il est intéressant de noter que dans le commentaire des articles de l'arrêté précité, les auteurs rappellent *« qu'il s'agit ici de donner une possibilité de conserver les images pendant trois mois et non d'une obligation et que ce délai de trois mois est un maximum. Il faut donc que la durée déterminée par le responsable du traitement se justifie au niveau de la proportionnalité. »*

[140] Tout en respectant les autres conditions exigées en cas de traitement sur base de l'article 6.1.f) du RGPD.
[141] Voir lignes directrices de la CNPD en matière de vidéosurveillance, mise à jour le 05/04/2024, page 14.
[142] Voir article 3 de l'arrêté royal du 6 décembre 2018 déterminant les lieux où le responsable du traitement peut diriger ses caméras de surveillance vers le périmètre entourant directement le lieu, conserver les images des caméras de surveillance pendant trois mois et donner accès en temps réel aux images aux services de police

- En France, les articles L251-1 et suivants du Code de la sécurité intérieure encadrent la mise en place de systèmes de vidéoprotection sur la voie publique par les autorités publiques compétentes pour diverses finalités, nécessitant notamment une autorisation du représentant de l'État dans le département, après avis de la commission départementale de vidéoprotection. Conformément à l'article L252-3 dudit Code, cette autorisation doit, entre autres, préciser la durée de conservation dans la limite d'un mois à compter de la transmission des images ou de l'accès aux enregistrements.

62. Sur base de ce qui précède, la CNPD conclut qu'une durée de conservation de six mois semble disproportionnée par rapport aux finalités listées à l'article 24.1 du projet de loi et elle recommande aux auteurs du projet de loi de s'inspirer des textes nationaux et étrangers précités.

Ainsi adopté à Belvaux
en date du 2 mai 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 8216 relative au droit de préemption en faveur de la promotion de l'habitat et modifiant 1° la loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu ; 2° loi modifiée du 22 octobre 2008 sur le droit d'emphytéose et le droit de superficie et introduisant différentes mesures administratives et fiscales en faveur de la promotion de l'habitat

Délibération n°26/AV11/2024
du 2 mai 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

2. Par courrier en date du 12 mai 2023, Monsieur le Ministre du Logement a invité la Commission nationale à se prononcer sur le projet de loi n°8216 relative au droit de préemption en faveur de la promotion de l'habitat et modifiant 1° la loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu ; 2° loi modifiée du 22 octobre 2008 sur le droit d'emphytéose et le droit de superficie et introduisant différentes mesures administratives et fiscales en faveur de la promotion de l'habitat (ci-après le « projet de loi »).

3. Il résulte de l'exposé des motifs que, au regard de l'augmentation du nombre de recours contentieux, le projet de loi vise à revoir les dispositions régissant le droit de préemption légal. Ainsi, il s'agit d'assurer la sécurité juridique, la transparence et la balance de tous les intérêts de la société afin que cet instrument de la politique du logement soit mieux accepté.

4. Le présent avis limitera ses observations aux aspects du projet de loi ayant trait à la protection des données à caractère personnel, et plus particulièrement aux dispositions de l'article 9 qui régissent la notification à effectuer par le notaire aux pouvoirs préemptant. La CNPD constate dans ce contexte que le projet de loi

n°8223[143] contient des dispositions quasi-identiques à celles de l'article 9 du projet de loi sous examen sans qu'elle ait toutefois été saisie pour avis pour le projet de loi n°8223.

I. Remarques liminaires

5. Il ressort de l'exposé des motifs du texte sous avis que le droit de préemption légal constitue un outil important de la mise en œuvre de la politique du logement. Il permet aux pouvoirs préemptant, à savoir les communes et le Fonds du Logement, d'acquérir, par préférence à tout autre acquéreur, un immeuble en vue de la réalisation de projets répondant à l'un des objectifs d'intérêt général énumérés à l'article 2 du projet de loi, tels que la réalisation de logements abordables.

6. En ce qui concerne l'exercice du droit de préemption, il appartient au notaire d'informer les pouvoirs préemptant de l'existence d'un projet d'acte en leur fournissant un certain nombre d'informations qui, si elles se rapportent à une personne physique identifiée ou identifiable, constituent des données à caractère personnel. Cette transmission de données personnelles par le notaire aux pouvoirs préemptant constitue une ingérence au droit à la protection de la vie privée et au droit à la protection des données à caractère personnel, tels que consacrés notamment par les articles 20 et 31 de la Constitution ainsi que les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

7. Il convient toutefois de rappeler que les droits au respect de la vie privée et à la protection des données ne sont pas des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société et être mis en balance avec d'autres droits fondamentaux[144]. Conformément aux articles 37 de la Constitution et 52.1 de la Charte, des limitations peuvent être apportées pourvu qu'elles soient prévues par la loi et respectent le contenu essentiel des droits fondamentaux ainsi que le principe de proportionnalité. En vertu de ce dernier principe, les limitations doivent s'opérer dans les limites du strict nécessaire et répondre effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et des libertés d'autrui.

II. La notification à effectuer par le notaire aux pouvoirs préemptant en vue d'un exercice éventuel du droit de préemption

8. Selon l'article 9 du projet de loi, il appartient au notaire de notifier, avant la passation de l'acte authentique, aux pouvoirs préemptant un certain nombre d'informations sur l'acte projeté. Ces informations sont à qualifier de données à caractère personnel si elles se rapportent à une personne physique identifiée ou identifiable, ce qui est notamment le cas si le propriétaire de l'immeuble faisant l'objet

[143] Projet de loi portant modification de la loi modifiée du 17 avril 2018 concernant l'aménagement du territoire et modifiant : 1. La loi modifiée du 16 août 1967 ayant pour objet la création d'une grande voirie e communication et d'un fonds de route ; 2. La loi modifiée du 15 mars 1979 sur l'expropriation pour cause d'utilité publique ; 3. La loi modifiée du 19 juillet concernant l'aménagement communal et le développement urbain

[144] CJUE, arrêt du 7 mars 2024, Endemol Shine Finland Oy, C-740/22, ECLI:EU:C:2024:216, point 52.

ANNEXES

de l'acte projeté est une personne physique. Les règles du RGPD ont alors vocation à s'appliquer.

9. Aux termes de l'article 6.1 du RGPD, un traitement de données n'est licite que si une des conditions y énumérées est remplie. En l'espèce, la transmission de données personnelles par le notaire aux pouvoirs préemptant est nécessaire au respect d'une obligation légale à laquelle le notaire est soumis, conformément à l'article 6.1.c) du RGPD. Le traitement des données personnelles par les pouvoirs préemptant est, quant à lui, nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont sont investis les pouvoirs préemptant, à savoir l'exercice éventuel du droit de préemption dans le cadre de la mise en œuvre de la politique du logement, conformément à l'article 6.1.e) du RGPD.

10. L'article 6.3 du RGPD prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de de l'autorité publique dont est investi le responsable du traitement. Il résulte de cette disposition que :

« Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par:
a) le droit de l'Union; ou
b) le droit de l'État membre auquel le responsable du traitement est soumis.
Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. 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. »

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[145].

11. La CNPD note favorablement que le projet de loi confère une base légale aux traitements de données effectués en

[145] V. en ce sens M. Besch, Normes et légistique en droit public luxembourgeois, Promoculture Larcier, 2019, n°619. V. entre autres CourEDH, arrêt du 4 décembre 2015, Zakharov ce. Russie, §§ 228 à 229 ; CourEDH, arrêt du 24 avril 2018, Benedik v. Slovenia, §§ 122 à 125

vertu du texte sous examen. Par ailleurs, l'instrument du droit de préemption semble répondre à un objectif d'intérêt public, à savoir la création de logements abordables, et être proportionné à cet objectif légitime poursuivl[146]. La Commission nationale estime néanmoins que certaines dispositions du projet de loi manquent de précision.

1. La transmission électronique des données personnelles

12. Alors que la loi actuellement en vigueur prévoit que la notification à effectuer par le notaire aux pouvoirs préemptant se fait par voie postale, et plus particulièrement par envoi recommandé[147], l'article 9 du projet de loi dispose que la notification sera effectuée dorénavant par voie électronique et qu'un accusé de transmission sera généré automatiquement.

13. Il est à regretter que ni les dispositions du texte en projet ni le commentaire des articles ne précisent la manière dont cette transmission électronique des données s'effectuera. Est-il prévu que cette transmission se fera par simple courriel ou de créer une plateforme destinée à permettre au notaire de transmettre aux pouvoirs préemptant les informations nécessaires ? Quel sera le fonctionnement d'une telle plateforme ? Qui sera en charge de l'opérer et qui sera à considérer comme responsable du traitement ? Se posent également dans ce contexte des questions de sécurité informatique. La CNPD invite les auteurs d'apporter les précisions nécessaires au projet de loi.

2. Les données personnelles faisant l'objet de la notification

14. Il résulte de l'article 9, alinéa 1er, du projet de loi que le notaire transmet aux pouvoirs préemptant une copie du compromis ou du projet d'acte. Par ailleurs, l'alinéa 3 dispose que le notaire veille à communiquer au moins les informations y énumérées, telles que l'identité et le domicile du propriétaire.

15. La Commission nationale se permet de rappeler l'importance du principe de minimisation des données consacré à l'article 5.1.c) du RGPD selon lequel les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Ce principe est lié au principe de proportionnalité en vertu duquel les limitations au droit à la protection des données personnelles doivent s'opérer dans les limites du strict nécessaire[148]. À cet égard, la CNPD s'interroge s'il est vraiment nécessaire de transmettre une copie de l'intégralité du compromis ou du projet d'acte aux pouvoirs préemptant. En effet, ces actes peuvent contenir des stipulations qui ne sont pas pertinentes pour la décision à prendre par les pouvoirs préemptant, de sorte que la transmission de telles informations est susceptible de contrevenir aux principes de minimisation des données et de proportionnalité.

[146] Cf. points 5 à 7 du présent avis.
[147] Art. 8 de la loi modifiée du 22 octobre 2008 portant sur le droit d'emphytéose et le droit de superficie et introduisant différentes mesures administratives et fiscales en faveur de la promotion de l'habitat.
[148] Cf. point 7 du présent avis.

ANNEXES

16. Par ailleurs, l'article 9, alinéa 3, du projet de loi comporte une énumération seulement exemplative (« au moins ») des informations à transmettre par le notaire aux pouvoirs préemptant. La Commission nationale estime qu'en application des articles 31 et 37 de la Constitution, les données que le notaire transmet aux pouvoirs préemptant doivent être limitativement énoncées au niveau de la loi[149]. La Commission nationale recommande dès lors de faire abstraction des termes « au moins » et d'indiquer précisément et de manière exhaustive les données qui sont à transmettre.

3. La durée de conservation

17. La CNPD note que le texte sous examen ne comporte pas de disposition fixant la durée de conservation des données traitées. Elle se permet de rappeler que les données collectées dans le cadre d'une mission légale ne doivent être conservées qu'aussi longtemps qu'elles sont nécessaires pour l'exécution de la mission voire de l'obligation légale pour laquelle elles ont été collectées[150]. Ainsi, si les auteurs décident de suivre la Commission nationale dans sa recommandation de préciser davantage le fonctionnement du mode de transmission par lequel le notaire effectuera les notifications[151], il pourrait être utile d'inclure une disposition spécifiant la durée de conservation des données transmises aux pouvoirs préemptant.

Ainsi adopté à Belvaux
en date du 2 mai 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[149] Cf. en ce sens: Avis 60.868 du Conseil d'État du 22 décembre 2023, doc. parl. n°7932/05, p. 7.
[150] Cf. en ce sens: Avis 61.688 du Conseil d'État du 22 décembre 2023, doc. parl. n°8324/05, p. 4.
[151] Cf. point 13 du présent avis.

6

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8148 relative à la rétention des données à caractère personnel et portant modification : 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État

Délibération n°28/AV12/2024
du 16 mai 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Par courrier en date du 2 février 2023, Madame la Ministre de la Justice a invité la Commission nationale à se prononcer sur le projet de loi n°8148 relative à la rétention des données à caractère personnel et portant modification: 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État (ci-après le « projet de loi »).

3. Selon l'exposé des motifs, le projet de loi a pour objet de *« répondre aux exigences de la jurisprudence européenne en permettant une conciliation entre les deux exigences que sont sécurité et liberté »*[152]. La Cour de justice de l'Union européenne (ci-après la « CJUE » ou la « Cour ») a depuis le premier arrêt en la matière en 2014[153] détaillé de plus en plus sa position quant à la possibilité pour les opérateurs de télécommunications ou les fournisseurs de services de communications électroniques (ci-après les « opérateurs et fournisseurs ») de conserver des données de trafic et de localisation et pour les autorités nationales compétentes d'accéder aux données ainsi conservées.

[152] Doc. parl. de dépôt, p. 17.
[153] Arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238.

ANNEXES

4. La Cour soulève qu'une telle conservation par les opérateurs et fournisseurs va à l'encontre du principe de confidentialité consacré par 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 (ci-après la « directive vie privée et communications électroniques »). Ainsi, les données de trafic et de localisation doivent en principe être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication.

5. Ce principe d'effacement subit pourtant des dérogations, notamment en ce qui concerne la conservation de données requises pour établir les factures et les paiements pour interconnexion, voire encore la possibilité avec le consentement de la personne concernée de traiter ces données à des fins commerciales ou de fourniture de services à valeur ajoutée. Une autre dérogation découle de l'article 15 de cette directive qui accorde la possibilité aux États membres de limiter la portée des droits et des obligations dans certains cas.

6. La jurisprudence en matière de rétention des données porte ainsi essentiellement sur l'interprétation de la Cour sur les dérogations possibles en application de l'article 15 de la directive vie privée et communications électroniques. Dans les arrêts[154] qui ont suivi le premier arrêt « Digital Rights Ireland » du 8 avril 2014, la Cour décline de plus en plus cette interprétation et fournit des indications quant aux modalités qui doivent accompagner ces dérogations admissibles au principe de confidentialité.

7. La CJUE détermine ainsi que l'article 15 de la directive vie privée et communications électroniques, lu à la lumière de la Charte des droits fondamentaux de l'Union européenne, ne s'oppose pas à des mesures législatives nationales prévoyant tant la conservation de données de trafic et de localisation que l'accès à ces données pour autant qu'elles soient limitées en ce qui concerne les objectifs recherchés ainsi que délimitées en ce qui concerne les personnes visées, les moyens de communications ciblés, les catégories de données conservées et la durée de conservation retenue et qu'elles *« assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus »*[155].

[154] Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970 ;
arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788 ;
arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791 ;
arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790 ;
arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152 ;
arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258 ;
arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702 ;
arrêt du 17 novembre 2022, Spetsializirana prokuratura C-350/21, EU:C:2022:896 ;
arrêt du 30 avril 2024, Procura della Repubblica presso il Tribunale di Bolzano, C-178/22, EU:C:2024:371 ;
arrêt du 30 avril 2024, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370.

[155] Voir arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702, point 132.

6

8. Au fil des dernières années, la CJUE a pu analyser, dans les arrêts relatifs à la rétention des données, différentes mesures législatives de conservation et d'accès ayant tenté de répondre aux exigences soulevées dans sa jurisprudence. Par conséquent, elle a pu préciser de plus en plus ce que des mesures législatives de conservation et d'accès doivent respecter afin d'être conformes au cadre légal en matière de protection des données à caractère personnel. L'exposé des motifs décrit extensivement la majorité des exigences soulevées par la CJUE.

9. De manière générale, la CNPD souhaite néanmoins rappeler que pour assurer la conformité au principe de proportionnalité, la CJUE a exprimé à plusieurs reprises que la conservation doit être limitée au strict nécessaire pour atteindre les objectifs. Dans ses arrêts, la CJUE procède de manière systématique pour analyser la proportionnalité des mesures.

10. Ainsi, en premier lieu, elle détermine les finalités recherchées par les mesures législatives de conservation ou d'accès. Cette première étape est essentielle, non seulement parce que les finalités sont listées de manière exhaustive[156] dans l'article 15 de la directive vie privée et communications électroniques, mais également parce que l'importance de l'objectif recherché a un impact sur l'ingérence tolérée sur la vie privée des personnes concernées. Force est de constater à la lecture des arrêts de la CJUE en matière de rétention de données que plus les objectifs sont importants, plus l'ingérence des mesures de conservation et d'accès dans la vie privée des personnes concernées est tolérée.

11. Il en résulte que l'étendue des mesures législatives de conservation et d'accès dépend largement de l'objectif recherché. Ainsi, une conservation généralisée et indifférenciée des données relatives au trafic peut être tolérée, sous réserve de respecter certaines conditions, pour les objectifs de préservation de la sécurité nationale. Or, pour la lutte contre la criminalité grave, il est nécessaire de limiter l'étendue des mesures de conservation ou d'accès sur base de critères objectifs et non discriminatoires. Cette limitation peut se rapporter aux personnes concernées, aux catégories de données, aux zones géographiques, voire encore aux moyens de communications utilisés. En matière de criminalité simple[157], la CJUE est encore plus exigeante.

12. En deuxième lieu, la CJUE apprécie tant la durée des mesures de conservation et d'accès que la durée de conservation des données proprement dites. En ce qui concerne la durée de conservation des données, la CJUE retient qu'elle doit être limitée au strict nécessaire pour atteindre l'objectif recherché[158] et être choisie sur base de critères objectifs[159]. En ce qui concerne la durée d'application des mesures, la CJUE ne s'est jusqu'à présent prononcée que sur les

[156] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 112.
[157] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, points 110 et 111.
[158] Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 63.
[159] Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 64, et arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 108.

ANNEXES

mesures concernant l'accès aux données conservées. Dans ce contexte, elle explique que l'accès *« présente en tout état de cause un caractère grave indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période, lorsque [...] cet ensemble de données est susceptible de permettre de tirer des conclusions précises sur la vie privée de la ou des personnes concernées »*[160], et qu'il doit se limiter au strict nécessaire[161].

13. Enfin, la CJUE exige que les mesures législatives permettent *« d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicite de ces données »*[162]. Ces garanties s'imposent non seulement pour les mesures législatives de conservation[163], mais également pour les mesures législatives d'accès[164] aux données stockées.

14. Selon l'exposé des motifs, le projet de loi sous avis a pour objet *« d'encadrer la conservation et l'usage des données de trafic et de localisation sans priver ces données de leur valeur utile, notamment en fixant des conditions strictes d'accès et de durée de conservation »*[165].

15. Pour ce faire, le projet de loi entend supprimer de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (dénommée ci-après la « loi Télécom ») l'obligation de conservation généralisée et indifférenciée de toutes les données de trafic et de localisation pour tous les objectifs énumérés à l'article 15 de la directive vie privée et communications électroniques. En tant que substitut, il entend introduire plusieurs mesures législatives de conservation des données et d'accès à ces données qui sont censées répondre aux exigences de la CJUE.

16. En droit interne, la Constitution garantit que les libertés publiques des citoyens sont respectées. Dans le contexte du présent projet de loi, ces sont notamment les libertés publiques consacrées aux articles 20 (vie privée), 30 (inviolabilité des communications) et 31 (protection des données) de la Constitution qui sont en jeu dans le cadre du présent projet de loi. De plus, l'article 37 de la Constitution dispose que *« [t]oute limitation de l'exercice des libertés publiques doit être prévue par la loi [...]»*.

17. Il importe encore de mentionner l'article 8.2 de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que la jurisprudence s'y

[160] Voir arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 39.
[161] Voir arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 38.
[162] Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 66.
[163] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 122, qui impose aux fournisseurs de service de communications électroniques une conservation des données sur le territoire de l'Union européenne.
[164] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 121, qui impose aux autorités d'informer les personnes concernées de l'accès, dans la mesure où cette information ne risque pas de compromettre les enquêtes menées.
[165] Doc. parl. de dépôt, p. 17.

rapportant. Cette disposition prévoit qu' *« [i]l 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 ».* Pour déterminer la conformité à l'article 8.2, la Cour européenne des droits de l'homme (ci-après la « CEDH ») recherche si l'ingérence est prévue par la loi, poursuit un/des but(s) légitime(s) et si elle est proportionnée à ce(s) but(s).

18. La CNPD ayant déjà abordé cet aspect, en particulier celui de la proportionnalité ainsi que de la prévisibilité de la loi dans d'autres avis, elle se limite à renvoyer à ces observations[166].

19. La CEDH admet néanmoins une atténuation pour le critère de prévisibilité de la loi en matière de surveillance secrète : *« La Cour a jugé à plusieurs reprises que, en matière d'interception de communications, la* « prévisibilité » *ne pouvait se comprendre de la même façon que dans beaucoup d'autres domaines. Dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la prévisibilité ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence »*[167].

20. Cette atténuation est applicable en matière de rétention des données, étant donné que la CEDH qualifie la conservation de données de trafic et de localisation comme une mesure de surveillance secrète dont le degré d'ingérence dans la vie privée des personnes concernées équivaut à celui de l'interception du contenu de la communication[168]. La conservation et l'accès aux données de trafic et de localisation doivent dès lors bénéficier des mêmes sauvegardes que les mesures de surveillance secrète[169]. Ainsi, *« [...] le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrète »*[170].

21. La CEDH ajoute encore que la loi doit, de manière suffisamment claire, définir l'étendue et les modalités de l'exercice du pouvoir d'appréciation de l'autorité qui

[166] Voir délibération n°3/AV3/2021 du 10 février 2021, Point II.2.
[167] Voir arrêt de la CEDH du 4 décembre 2015, Roman Zakharov c. Russie, point 229.
[168] Voir arrêt de la CEDH du 11 janvier 2022, Ekimdzhiev et autres c. Bulgarie, point 394.
[169] *Ibid*, point 295.
[170] Voir arrêt de la CEDH du 4 décembre 2015, Roman Zakharov c. Russie, point 229.

ANNEXES

ordonne la mesure de surveillance pour éviter l'arbitraire. Elle *« énonce les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements »*[171].

22. Concernant la condition que la mesure doit être nécessaire dans une société démocratique, la CEDH précise que des garanties adéquates et effectives doivent exister afin d'éviter l'arbitraire et les abus. Elle estime que l'existence d'un contrôle de la nécessité de la mesure est une telle garantie et que l'appréciation doit se faire en prenant en compte toutes les circonstances de l'affaire en question. La CEDH explique encore que le contrôle peut se faire à trois moments : au moment où la mesure est ordonnée, pendant l'exécution et lorsque la mesure est terminée.[172]

23. Afin d'apprécier si les différentes mesures législatives prévues par le projet de loi respectent les exigences de la CJUE et de la CEDH, il est nécessaire de différencier entre les mesures législatives de conservation de données (I) et les mesures législatives d'accès à ces données (II). Enfin, il convient encore d'examiner les autres modifications (III) que le projet de loi entend apporter.

XIX. Les mesures législatives de conservation de données

24. Le projet de loi opère un changement de paradigme en ce qu'il introduit le principe de l'interdiction d'une conservation généralisée et indifférenciée des données de trafic et de localisation. Il ressort du commentaire des articles que *« [c]ontrairement au libellé introduit par la Loi Telecom [...] le principe inscrit au nouveau paragraphe 1er est celui de l'interdiction de conservation des données relatives au trafic. Tel que prévu par la jurisprudence européenne, les données seront donc effacées ou rendues anonymes sur base du principe de nécessité et tel que préconisé par la CJUE ».*

25. Il est effectivement de jurisprudence constante que le principe de confidentialité est d'interprétation stricte[173]. Ainsi, la Cour a pu confirmer à plusieurs reprises qu'une dérogation à ce principe sur base de l'article 15 de la directive vie privée et communications électroniques ne peut pas, en ce qui concerne notamment la conservation de ces données, devenir la règle mais doit toujours rester l'exception et doit respecter le principe de nécessité.

26. La CJUE fournit dans ses arrêts les exigences à prendre en compte afin de garantir une conservation limitée au strict nécessaire. Ces délimitations peuvent jouer

[171] *Ibid.*, points 230 et 231.
[172] *Ibid.*, points 232 à 234.
[173] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 89.

au niveau des finalités et/ou de l'étendue de la mesure. Etant donné que l'exposé des motifs reprend fidèlement les exigences que la CJUE a rattaché à chacune de ces catégories, le présent avis se limite à renvoyer à ces explications[174].

27. La CJUE répartit les mesures législatives de conservation des données en trois grandes catégories, à savoir la conservation ciblée, la conservation généralisée et indifférencié et la conservation rapide.

28. À la lecture du projet de loi, il devient clair que les auteurs introduisent ces trois catégories de mesures, dont certaines doivent être ordonnées (A) par le juge d'instruction, le procureur ou le service de renseignement (ci-après le « SRE ») tandis que d'autres résultent d'une obligation légale de conservation (B).

29. De plus, la CJUE exige que la conservation des données de trafic et de localisation soit entourée de garanties suffisantes et appropriées par les opérateurs et fournisseurs. Comme chaque mesure de conservation doit répondre à cette exigence, il convient de regrouper les observations y relatives dans une section dédiée (C).

1. Les mesures de conservation devant être ordonnées

1. La mesure de conservation du nouvel article 24-3 du Code de procédure pénale

30. L'article 1er, point 1° du projet de loi introduit un nouvel article 24-3 dans le Code de procédure pénale (ci-après le « CPP ») ayant comme objectif de mettre à la disposition du procureur d'État une mesure de conservation des données de trafic et de localisation. Ainsi, le procureur d'État peut ordonner dans le cadre de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement la conservation des données relatives au trafic et à la localisation qu'il juge nécessaires.

31. La CNPD partage la confusion exprimée par les Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun en ce qu'il n'est pas clair si la mesure de conservation vaut pour les données déjà générées ou traitées par les opérateurs et fournisseurs ou si elle vaut pour les données qui seront encore générées ou traitées par les opérateurs et fournisseurs à partir de la date de l'ordonnance[175]. Le commentaire des articles contribue davantage à la confusion comme les auteurs du projet de loi parlent tant de la mesure comme conservation ciblée que *« d'une sorte de « quick freeze »* [conservation rapide] *pour le futur »*[176]. Ainsi, il n'est pas tout à fait clair si la nouvelle mesure est une mesure de conservation ciblée ou une mesure de conservation rapide.

32. D'après la compréhension de la CNPD, la conservation ciblée ainsi que la conservation

[174] Doc. parl. de dépôt, p. 11 à 15.
[175] Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.3.
[176] oc. parl. de dépôt, p.18.

ANNEXES

rapide telles que décrites par la CJUE sont deux mesures législatives distinctes, avec notamment des exigences distinctes. En effet, pour la conservation rapide, la CJUE exige notamment que *« [d]ans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu »*[177]. Cette exigence s'explique par le fait que le traitement initial des opérateurs et fournisseurs avait une finalité commerciale. Or, après l'ordonnance de conservation rapide, une nouvelle finalité s'ajoute à cette finalité initiale. Cette nouvelle finalité de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, devrait dès lors être ancrée dans la loi.

33. Enfin, d'après la description fournie par la CJUE, la conservation rapide devrait servir à conserver les données dont il existe un risque de perte ou de modification. Il s'agit donc d'une mesure qui s'applique à des données existantes et déjà détenues par les opérateurs et fournisseurs, plutôt qu'à des données qui seront générées ou traitées dans le futur[178]. Ainsi, la CNPD se demande si le nouvel article 24-3 du CPP ne se limite pas à introduire une conservation ciblée plutôt qu'une conservation rapide.

34. Tel que revendiqué par les Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun, des clarifications quant à la mesure législative visée par l'article 24-3 du CPP devraient être apportées, notamment pour préciser si elle se rapporte aux données déjà générées ou traitées, et/ou aux données qui seront générées ou traitées dans le futur[179]. Si effectivement les auteurs du projet de loi visent les deux cas de figure, c'est-à-dire les données futures et les données existantes, se pose alors la question s'il ne serait pas plus clair de prévoir deux dispositions séparées.

35. Par ailleurs il serait intéressant de savoir pourquoi les auteurs du projet de loi n'ont pas rajouté la mesure de conservation ciblée à l'article 24-1 du CPP régissant la « mini-instruction ». D'autant plus qu'un contrôle juridictionnel effectif serait alors garanti et qu'un lien avec l'article 67-1 du CPP traitant de l'accès aux données ainsi conservées serait établi. D'après la compréhension de la CNPD, il ressort des travaux parlementaires de l'article 67-1 du CPP que le juge d'instruction peut ordonner l'accès aux données conservées par les opérateurs et fournisseurs ainsi que la conservation de données futures. Le recours à la mini-instruction serait dès lors envisageable, à condition que l'article 67-1 du CPP respectent les exigences de le CJUE.

[177] Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 164 et arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 87.
[178] Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 162 et 163.
[179] Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.3.

36. Dans le même ordre d'idées, la CNPD se demande pourquoi les auteurs du projet de loi, si la mesure sous avis devrait être une mesure de conservation rapide, ne l'ont pas ajoutée au Chapitre X du CPP prévoyant la conservation rapide des données informatiques à disposition du juge d'instruction et du procureur d'État.

37. Dans tous les cas, les mesures législatives doivent répondre aux exigences de la CJUE. Partant, dans l'hypothèse où le nouvel article 24-3 du CPP régit une mesure de conservation ciblée des données de trafic et de localisation, elle ne peut être prise qu'*« aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique »*[180]. Par ailleurs, elle doit être *« délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable »*[181]. La Cour précise encore qu'une telle mesure doit assurer, *« par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus »*[182].

38. Concernant les finalités pour lesquelles on peut recourir à une mesure de conservation ciblée, la jurisprudence de l'Union européenne admet que ce n'est possible qu'*« aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique »*[183].

39. Il y a lieu de constater que le nouvel article 24-3 du CPP retient un seuil comme critère de délimitation, à savoir les infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement. La CNPD partage l'appréciation du Conseil d'État que *« les infractions sanctionnées par une peine d'emprisonnement égale ou supérieure à un an ne relevant de surcroît pas toutes de la criminalité grave »*[184]. Ainsi, il convient de se demander si le seuil fixé est suffisamment élevé. La CNPD réitère dès lors sa préférence exprimée dans plusieurs avis[185] pour une liste limitative d'infractions qualifiées de graves. Une liste limitative permettrait de réserver les mesures législatives aux enquêtes et aux actes de poursuite relatifs à des infractions qui se situent clairement dans le contexte de la criminalité grave.

40. Les auteurs du projet de loi expliquent qu'il s'agit d'un choix politique national comme la notion ne connaît pas de définition harmonisée au niveau de l'Union européenne[186]. Dans un arrêt récent, la

[180] Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 168.
[181] *Ibid.*
[182] *Ibid.*
[183] *Ibid.*
[184] Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.4.
[185] Voir par exemple avis n°85/2010 du 24 avril 2010 et avis n°214/2014 du 13 mai 2014.
[186] Doc. parl. de dépôt, p.20 et suivants.

ANNEXES

CJUE confirme cette approche[187] toute en rappelant que *« la définition des « infractions graves », opérée par les États membres, doit respecter les exigences qui découlent de cet article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte »*[188].

41. À cet égard, la Cour souligne que *« les États membres ne sauraient dénaturer la notion d'*« infraction grave » *et, par extension, celle de* « criminalité grave »*, en y incluant, aux fins de l'application de cet article 15, paragraphe 1, des infractions qui ne sont manifestement pas graves, au regard des conditions sociétales prévalant dans l'État membre concerné, alors même que le législateur de cet État membre a prévu de les punir d'une peine maximale de réclusion de trois ans »*[189].

42. Même si la Cour ne propose pas de définition pour les notions d'« infraction grave » ou de « criminalité grave », elle donne néanmoins des considérations à prendre en compte par les États membres. Ainsi, la Cour ne rejette pas le concept que la gravité de l'infraction est déterminée par un seuil[190]. En effet, la Cour estime qu'un seuil fixé par la loi est un critère objectif permettant de déterminer le degré de gravité d'une infraction.

43. Or, la Cour soulève également que le seuil choisi par les États membres *« ne doit pas être à ce point large que l'accès à ces données devienne la règle plutôt que l'exception »*[191]. Elle ajoute que la notion de « criminalité grave » ou d'« infraction grave », ne doit pas *« couvrir la grande majorité des infractions pénales, ce qui serait le cas si le seuil au-delà duquel la peine de réclusion maximale dont est punie une infraction justifie que celle-ci soit qualifiée d'infraction grave était fixé à un niveau excessivement bas »*[192].

44. Toujours en ce qui concerne la détermination des infractions graves par un seuil, la Cour soulève encore que *« par référence non pas à une peine minimale applicable mais à une peine maximale applicable, il n'est pas exclu qu'un accès à des données, constitutif d'une ingérence grave dans les droits fondamentaux, puisse être demandé à des fins de poursuites d'infractions ne relevant pas, en réalité, de la criminalité grave »*[193]. Elle estime néanmoins que ceci n'est *« pas nécessairement contraire au principe de proportionnalité »*[194].

45. Afin d'apprécier si la proportionnalité est garantie lorsqu'un seuil fait référence à une peine maximale, la CJUE estime qu'il faut veiller à deux choses. Premièrement, il convient de vérifier si la disposition législative vise de *« manière générale l'accès aux données conservées [...]*

[187] Arrêt du 30 avril 2024, Procura della Repubblica presso il Tribunale di Bolzano, C-178/22, EU:C:2024:371, points 44 à 47.
[188] *Ibid.*, point 47.
[189] *Ibid.*, point 50.
[190] *Ibid.*, point 54.
[191] *Ibid.*, point 55.
[192] *Ibid.*
[193] *Ibid.*, point 57.
[194] *Ibid.*, point 58.

sans préciser la nature de ces données »[195]. La Cour estime que s'il n'est pas précisé dans la disposition quelles données sont accédées et que ceci est à la libre appréciation des autorités demandant l'accès, il est possible que la mesure en question ne se limite pas aux infractions graves. Effectivement, si l'autorité se limite à demander l'accès à des données ne permettant pas des conclusions précises sur la vie privée des personnes concernées, cet accès ne peut pas être qualifié de grave et est possible pour les infractions dites simples[196].

46. Il en résulte que, deuxièmement, une juridiction ou une entité administrative indépendante intervenant dans le cadre du contrôle préalable doit apprécier le degré de gravité de l'ingérence dans la vie privée par rapport à la gravité de l'infraction. Lorsqu'il découle de ce contrôle préalable que le degré d'ingérence dans la vie privée n'est pas proportionnée au degré de l'infraction, la juridiction ou l'autorité administrative *« doit être habilitée à refuser ou à restreindre cet accès »*[197] car cette entité *« doit être en mesure d'assurer un juste équilibre entre, d'une part, les intérêts légitimes liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès »*[198].

47. Dans la mesure où le projet de loi sous avis entend délimiter la criminalité grave de la criminalité simple par référence à un seuil de peine maximale, les critères énoncés par la CJUE doivent être pris en considération. Or, comme cette jurisprudence de la CJUE est postérieure au dépôt du projet de loi, il serait judicieux de revoir les mesures législatives prévues et de les conformer, le cas échéant, aux exigences de la CJUE. En ce qui concerne le seuil fixé, il peut, tel que déjà susmentionné, être remis en doute s'il est suffisamment élevé. Ensuite, en ce qui concerne le principe de proportionnalité, il convient de vérifier pour chaque mesure individuellement si les critères soulevés par la CJUE sont prévus.

48. La CNPD souhaite encore attirer l'attention du législateur au règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) 1077/2011, (UE) 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 qui dans son article 3.1. point 16 définit l'infraction pénale grave comme *« une infraction qui correspond ou est équivalente à l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI, si elle est passible, en droit national, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans ».* La CNPD se demande dès lors si cette définition ne pourrait pas servir de source d'inspiration pour le projet de loi sous avis.

[195] *Ibid.*, point 59.
[196] *Ibid.*
[197] *Ibid.*, point 60.
[198] *Ibid.*, point 61.

ANNEXES

49. Ensuite, en ce qui concerne l'étendue de la mesure législative prévoyant la conservation ciblée, la CJUE exige qu'elle soit prévue dans la loi nationale et limitée par des critères objectifs et non discriminatoires[199]. Or, il y a lieu de constater que la rédaction actuelle de l'article 24-3.1 alinéa 3 du CPP se limite à prévoir que la décision écrite et motivée du procureur d'État contient « *b) [l]'indication précise d'un ou de plusieurs des éléments suivants : la ou les personnes, les moyens de communications ou les lieux qui font l'objet de la conservation* ». La disposition ne contient pas de critères permettant de délimiter exactement les personnes, lieux ou moyens de communication à viser par la conservation.

50. Dans la mesure où le futur article 24-3 du CPP prévoit une conservation ciblée, la CNPD se demande dès lors s'il ne devrait pas contenir des critères permettant de délimiter les zones géographiques ou les personnes pouvant être visées par la mesure tel que préconisé par la CJUE ou encore la CEDH. Les auteurs du projet de loi auraient pu s'inspirer des éléments fournis par la Cour dans ses arrêts successifs[200] ainsi que des critères prévus au nouvel article *5bis* de la loi Télécom.

51. La Cour clarifie par ailleurs qu'à part une délimitation des personnes ou zones visées par la mesure, « *d'autres critères, objectifs et non discriminatoires, puissent entrer en ligne de compte afin d'assurer que la portée d'une conservation ciblée soit limitée au strict nécessaire et d'établir un lien, au moins indirect, entre les actes de criminalité grave et les personnes dont les données sont conservées. Cela étant, l'article 15, paragraphe 1, de la directive 2002/58 visant des mesures législatives des États membres, c'est à ces derniers et non à la Cour qu'il incombe d'identifier de tels critères, étant entendu qu'il ne saurait être question de réinstaurer, par ce biais, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation* »[201]. Il existe donc éventuellement d'autres critères non énumérés par la CJUE qui pourrait servir pour délimiter l'étendue de la mesure.

52. Concernant les catégories de données qui peuvent potentiellement être conservées, le futur article 24-3.1 alinéa 2 du CPP prévoit qu'un règlement grand-ducal « *détermine les catégories de données relatives au trafic susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuit d'infractions visées ci-dessus* ». La CNPD se rallie aux observations du Conseil d'État à ce sujet[202]. Elle ajoute que la jurisprudence de la CJUE énonce que pour la conservation ciblée, il appartient à la loi de contenir les critères objectifs et non discriminatoires qui permettent de déterminer quelles catégories de données peuvent être conservées. Il ne suffit dès lors pas de fixer les catégories de données qui peuvent être collectées, mais

[199] Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 76.
[200] Voir en ce sens par exemple, l'arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702, points 104 à 113.
[201] Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 83.
[202] Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.4 et 5.

il faut bien prévoir des critères sur base desquels on limite au strict nécessaire les données pouvant être collectées.

53. Par ailleurs, il ne ressort pas clairement de la disposition que le règlement grand-ducal visé correspond à celui pris initialement sur base de l'article 5 de le loi Télécom, à savoir le règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics. À l'instar des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun[203], la CNPD est d'avis qu'il doit être clair à la lecture de l'article 24-3 du CPP quel règlement grand-ducal est visé.

54. Concernant le règlement grand-ducal proprement dit, la CNPD est d'avis que sa rédaction devrait être adapté au nouveau régime. Le libellé de l'article 3 dudit règlement reflète dès lors toujours la logique d'une obligation légale de conservation généralisée et indifférenciée des données listées. La CNPD estime pourtant que le règlement grand-ducal devrait contenir une liste exhaustive de données qui constituent des données de trafic ou de localisation parmi lesquelles le procureur d'État doit choisir sur base de critères objectifs et non discriminatoires prévus par la loi celles qui sont nécessaires à la réalisation de son objectif.

55. Dans le même ordre d'idée, il convient de se demander pourquoi les auteurs ont choisi d'inclure dans le paragraphe 1er alinéa 2, les appels infructueux. En effet, déjà en 2010 lorsque ce concept a été introduit dans la loi Télécom, le Conseil d'État avait constaté que cette précision était superflue car « *peu importe si un appel est fructueux ou infructueux, il constitue une donnée du trafic* »[204].

56. Par ailleurs, tel qu'expliqué par les Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun[205], il reste à clarifier si le contrôle juridictionnel existant pour l'ordonnance du procureur d'État respecte les exigences de la CJUE[206] ou encore de la CEDH[207] en la matière.

57. Ensuite, en ce qui concerne la durée de conservation retenue, l'article 24-3 du CPP prévoit une durée de 6 mois, prolongeable si nécessaire. Or, il y a lieu de constater que le projet de loi ne prévoit pas de durée d'application de la mesure. Il est dès lors impossible de déterminer le moment à partir duquel il faut compter les 6 mois de durée de conservation. La CNPD se demande par conséquent si la disposition ne devrait pas être complétée par une durée d'application de la mesure, prévoyant ainsi la période sur laquelle les opérateurs et fournisseurs doivent procéder à la conservation. Une fois que la durée d'application de la mesure

[203] Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.2.
[204] Avis du Conseil d'État sur le projet de loi n°6113 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle, doc. parl. 6113/06, p.3.
[205] Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.3.
[206] Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 85, et jurisprudence citée.
[207] Voir arrêt de la CEDH du 11 janvier 2022, Ekimdzhiev et autres c. Bulgarie, point 301.

ANNEXES

prend fin, la durée de conservation des données commence à courir.

58. En ce qui concerne la durée de conservation proprement dite, à savoir 6 mois prolongeable, la CNPD regrette que les auteurs du projet de loi n'aient pas fourni d'explication quant au choix retenu. Elle se voit dès lors dans l'impossibilité d'apprécier la proportionnalité de la durée choisie. La CNPD se rallie par ailleurs au Conseil d'État. La Haute Corporation soulève en effet que la disposition *« est en outre source d'insécurité juridique étant donné qu'une prolongation d'un délai, contrairement à sa reconduction, ne donne pas de limite précise à la mesure, entraînant de ce fait une imprécision quant à sa durée »*[208].

59. Concernant la destruction des données à la fin de la durée de conservation prévue au paragraphe 2 du nouvel article 24-3 du CPP, il convient de soulever que la disposition prête à confusion. En effet, il semble que cette disposition reflète une obligation pour les opérateurs et fournisseurs en ce qu'ils doivent détruire les données une fois la durée de conservation venue à échéance. Or, comme l'article 24-3 du CPP encadre une mesure d'enquête préalable à disposition du procureur d'État, il ne ressort pas naturellement du texte que l'obligation de destruction s'adresse aux opérateurs et aux fournisseurs.

60. Ensuite, il convient de s'interroger sur l'exception au principe de destruction introduite par la deuxième partie de la phrase unique constituant le paragraphe 2 de l'article 24-3 du CPP. Ainsi, les données conservées au titre de l'article 24-3 du CPP auxquelles les autorités compétentes ont accédé ou qu'elles ont préservées ne sont pas détruites. Se pose alors la question de la durée de conservation ultime pour les données qui seront malgré tout conservées. De plus, la CNPD s'interroge sur la raison de cette conservation supplémentaire. Si les autorités compétentes ont préservé les données conservées utiles pour l'enquête, quelle est la raison pour laquelle les opérateurs et fournisseurs doivent les conserver au-delà de la durée initiale ? Il en va de même pour les données qu'ils ont accédées mais qu'ils n'ont pas jugé utiles pour préserver. Pourquoi les opérateurs et fournisseurs doivent les conserver ?

61. De plus, l'article 24-3 du CPP dans sa rédaction actuelle ne contient pas d'indication ou de référence vers la ou les dispositions encadrant l'accès aux données conservées. La CNPD se rallie à l'observation des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun[209] qu'une référence à l'article 67-1 du CPP qui selon les auteurs du projet de loi constitue le fondement de l'accès devrait être introduite.

62. De manière similaire, la CNPD s'interroge sur le renouvellement prévu par l'article 24-3.1 alinéa 3 point c) du CPP. Ne s'agit-il pas plutôt d'un renouvellement de la durée d'application de la mesure que de la durée de conservation des données stockées par

[208] Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.4.
[209] Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.2.

les opérateurs et fournisseur ? Une précision à cet égard serait souhaitable.

63. De plus, à l'instar du Parquet général[210] et du Conseil d'État[211], la CNPD se demande quelles conditions de forme et de fond devraient être remplies afin d'obtenir une prolongation de ce délai.

64. Enfin, l'article 24-3.1 alinéa 4 du CPP prévoit qu'en cas d'urgence, le procureur d'État peut ordonner verbalement la mesure de conservation et devra par la suite la confirmer dans les meilleurs délais par écrit dans la forme prévue à l'alinéa 3. Il convient de s'interroger s'il ne serait pas utile de prévoir un délai maximal précis pour le procureur d'État de confirmer sa décision orale.

2. La mesure de conservation de l'article 67-1 du Code de procédure pénale

65. Selon l'exposé des motifs, *« [l]'obligation de conservation des données de trafic et de localisation relatives aux communications électroniques a été introduite dans la législation luxembourgeoise par la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications ».* Toujours selon l'exposé des motifs, *« [l]es opérateurs nationaux sont donc tenus à conserver les données de trafic et de localisation au sens des articles 5 et 9 de la Loi Telecom et l'accès à ces données est garanti au juge d'instruction moyennant l'article 67-1 du Code de procédure pénale [...] ».*

66. L'article 67-1 du CPP semble donc régir uniquement l'accès aux données conservées et non pas la conservation des données proprement dite. Or, les travaux parlementaires de la loi ayant introduit l'article 67-1 dans le Code de procédure pénale expliquent que la mesure de repérage *« peut viser aussi bien les communications passées que les communications futures »*[212]. Le Conseil d'État avait soulevé dans son avis à l'époque que le repérage *« ne devrait viser que l'obtention de données d'appel déjà transmises »*[213], ce notamment pour que le repérage ne puisse pas être confondu avec l'écoute et être vu comme une sorte de « mini-écoute ». Bien que la commission parlementaire précise que l'écoute téléphonique se fait en temps réel, notamment pour intercepter les communications et enregistrer leur contenu et que dans le cadre du repérage *« on constate simplement qu'il y a eu un appel et on essaye de localiser tant l'origine que la destination de l'appel sans qu'il soit possible d'en connaître le contenu – ni même, comme il a déjà été relevé ci-dessus, le véritable auteur »*[214], il n'en reste pas moins que la question de savoir si l'article 67-1 du CPP pourrait servir au juge d'instruction pour ordonner une conservation des données n'a pas trouvé de réponse explicite.

67. La disposition en question autorise le juge d'instruction de procéder *« au repérage des données d'appel de moyens de télécommunication à partir desquels*

[210] Avis du Parquet général du 13 mars 2023, doc. parl. n°8148/02, p.6.
[211] Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.5.
[212] Voir travaux parlementaires du projet de loi n°4889, document de dépôt p.4.
[213] Avis du Conseil d'État du 19 mars 2002, doc. parl. n°4889/01, p.3.
[214] Rapport de la Commission juridique du 2 octobre 2002, doc. parl. 4889/03, p.3.

ANNEXES

ou vers lesquels des appels sont adressés ou ont été adressés »[215]. La terminologie choisie semble indiquer que le juge d'instruction peut ordonner la conservation des données qui seront encore générées. L'avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch[216] soutient ce point de vue. Si tel est le cas, le juge d'instruction peut donc par le biais de l'article 67-1 du CPP ordonner une conservation des données de trafic et de localisation.

68. Au vu de l'exposé de motifs, il semble que les auteurs du projet de loi n'ont pas abordé l'article sous cet angle, mais uniquement d'un point de vue d'accès aux données conservées. La CNPD se demande dès lors si l'article ne devrait pas être analysé et le cas échéant adapté afin de répondre aux exigences de la CJUE par rapport aux mesures ciblées de conservation de données.

69. Ainsi, en ce qui concerne la possibilité d'ordonner la conservation des données, l'article devra viser la finalité appropriée, contenir les conditions et critères pour délimiter l'étendue ainsi que prévoir des durées d'application et de conservation adéquates.

70. L'article 67-1 du CPP est d'ores et déjà applicable pour les faits qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement. La CNPD se limite à renvoyer à ses observations soulevées au points 39 à 47 du présent avis.

71. La CJUE exige encore qu'il existe dans la loi des critères permettant de limiter l'étendue des mesures de conservation. Selon la CJUE, la mesure de conservation peut être « *limitée soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave* »[217]. Force est de constater que les modifications apportées à l'article 67-1 du CPP ne prévoient pas de tels critères, de sorte que la CNPD est à se demander si les exigences de la CJUE sont respectées.

72. La disposition sous examen contient une durée d'application de la mesure qui doit être précisée par le juge d'instruction sans qu'elle puisse excéder un mois. Or, elle néglige de fixer une durée de conservation des données de trafic et de localisation par les opérateurs et fournisseurs. Il est néanmoins essentiel de prévoir une telle durée de conservation qui doit par ailleurs être limitée au strict nécessaire par rapport au but recherché.

73. Se pose encore la question générale si la durée de conservation devrait être fixée par les dispositions qui régissent les mesures

[215] Article 67-1, paragraphe 1er, point 1. du CPP dabs sa version actuelle.
[216] Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.4.
[217] Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 144.

de conservation. En effet, la durée de conservation des données est une obligation qui s'adresse *in fine* aux opérateurs et aux fournisseurs. Ne serait-il dès lors pas plus logique de prévoir une disposition sur les durées de conservation des données ordonnées par les juridictions, qui seront appropriées en fonction de la mesure ordonnée dans la loi Télécom ? Dans tous les cas, il doit découler clairement du texte que la durée de conservation s'adresse aux opérateurs et fournisseurs.

74. En dernier lieu, la CNPD se demande si une séparation des mesures de conservation et d'accès ne serait pas une alternative envisageable. Ceci dans un souci d'éviter toute confusion entre les mesures et de rendre plus lisibles les règles qui entourent ces deux mesures.

3. La mesure de conservation du nouvel article 7-1 de la loi SRE

75. L'article 3 point 2° du projet de loi introduit un nouvel article 7-1 dans la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement (ci-après la « loi SRE »). Cet article permet au SRE d'ordonner aux opérateurs et fournisseurs *« la conservation généralisée et indifférenciée des données relatives au trafic y compris l'identification des correspondants et de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés ».*

76. La CJUE admet une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation dans des situations particulières. À cet égard, elle explique que *« la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme »*[218].

77. La Cour admet dès lors que *« l'importance de l'objectif de sauvegarde de la sécurité nationale [...] dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux*

[218] Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 135.

ANNEXES

plus graves que celles que pourraient justifier ces autres objectifs »[219].

78. Selon la CJUE, la conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, qui est une ingérence particulièrement grave dans la vie privée des personnes, est donc possible si l'enjeu est la sécurité nationale. La mesure doit néanmoins être encadrée. Ainsi, la Cour considère que la menace grave doit être *« réelle et actuelle ou prévisible »*[220]. Bien que le nouvel article 7-1.1 de la loi SRE reprenne exactement ces termes, il n'est pas précisé sur base de quels critères et conditions une menace est considérée comme réelle et actuelle ou prévisible. La CNPD se demande dès lors si ces critères ne devraient pas être prévus par la loi, vu qu'une telle conservation constitue une ingérence particulièrement grave dans la vie privée des personnes concernées et qu'en vertu de l'article 52 de la Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») et de l'article 8.2 de la Convention des droits de l'homme toute limitation de l'exercice des droits et libertés doit être prévue par la loi. Même si la CEDH admet une certaine flexibilité dans la prévisibilité de la loi en matière de surveillance secrète pour préserver la sécurité nationale[221], il n'en reste pas moins que *« [...] le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrète »*[222].

79. Aux dispositions de la Charte s'ajoutent encore celles de la Constitution. Pour rappel, ce sont en effet les droits prévus aux articles 20 (vie privée), 30 (inviolabilité des communications) et 31 (protection des données) qui sont en jeu dans le cadre du présent projet de loi. Or, conformément à l'article 37 de la Constitution *« [t]oute limitation de l'exercice des libertés publiques doit être prévue par la loi [...]».*

80. Se basant sur les constatations ci-avant, la CNPD se demande par ailleurs si la disposition est suffisamment précise quant à l'étendue de la conservation. L'utilisation de la notion « conservation généralisée et indifférenciée » ne permet pas à elle seule de savoir de quelles données, de quelles zones, de quelles personnes, voire encore de quels moyens de communication on parle. Selon sa compréhension, on entend par « conservation généralisée et indifférenciée » le stockage de toutes les données de trafic et de localisation générées par tous les moyens de communication de la quasi-totalité de la population sur tout le territoire du pays.

[219] *Ibid*, point 136.
[220] *Ibid*, point 137.
[221] Voir points 16 à 19 du présent avis.
[222] Voir arrêt de la CEDH du 4 décembre 2015, Roman Zakharov c. Russie, point 229.

81. En ce qui concerne en particulier les catégories de données visées, la prévisibilité de la loi peut être remise en question. Dans le régime actuel, le règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics décrit quelles données seront conservées. Les catégories de données conservées sont dès lors connues.

82. Or, comme le nouveau régime de conservation à la disposition du SRE se réfère uniquement *« à la conservation généralisée et indifférenciée des données relatives au trafic y compris l'identification des correspondants et de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés »*, il ne ressort pas de manière suffisamment claire du texte de quelles données on parle exactement. La loi SRE ne contient pas de définition de ce qu'il faut entendre par une donnée relative au trafic ou à la localisation, et les définitions fournies par la loi Télécom[223] semblent également insuffisantes.

83. À l'instar de ce qu'elle a soulevé aux points 53 et 54 du présent avis, la CNPD estime qu'au moins un règlement grand-ducal devrait définir précisément quelles catégories de données constituent toutes les données de trafic et de localisation.

84. En ce qui concerne la durée de conservation, la CNPD constate à nouveau une confusion entre la durée de conservation des données et la durée d'application de la mesure. En effet, la durée de six mois prévue au nouvel article 7-1 (4) semble plutôt être une durée d'application de la mesure qu'une durée de conservation proprement dite. Il conviendrait dès lors d'ajouter une durée de conservation des données, car les opérateurs et fournisseurs doivent savoir pendant combien de temps ils doivent conserver les données une fois que la mesure prend fin.

85. L'article 7.2 de la loi SRE continue à régler l'accès aux données conservées au titre des articles 7-1 et 7-2 de la loi SRE. La CNPD se félicite qu'une référence explicite à l'article encadrant l'accès aux données soit incluse.

4. Les mesures de conservation du nouvel article 7-2 de la loi SRE

86. L'article 3 point 3° du projet de loi introduit un nouvel article 7-2 dans la loi SRE permettant à ce dernier d'enjoindre deux sortes de mesures : la conservation rapide et la conservation ciblée des données de trafic et de localisation.

[223] Article 2 de la loi Télécom:
(...)
(f) «données relatives au trafic»: toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation;
(g) «données de localisation»: toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;
(...)

ANNEXES

87. Tel que soulevé aux points 31 et suivants du présent avis, les mesures de conservation rapide et de conservation ciblée ne couvrent pas les mêmes situations et ne sont pas soumises aux mêmes exigences. Il convient dès lors à apprécier les deux mesures séparément.

a. La conservation ciblée des données de trafic et de localisation

88. En ce qui concerne l'étendue de la mesure de conservation ciblée, la CJUE exige que la loi prévoie les critères objectifs et non discriminatoires qui permettent de déterminer les catégories de données pouvant être collectées.

89. Le projet de loi se limite à renvoyer à l'article 4 de la loi SRE qui consacre le principe général de la proportionnalité et de nécessité des mesures à prendre par le SRE. Le libellé de l'article 4 de la loi SRE ne semble en effet pas suffisamment précis pour limiter l'étendue de la mesure, car il ne fait que consacrer un principe général sans qu'il contienne des critères pour limiter la mesure de conservation ciblée à des personnes, des endroits ou des moyens de communications. Le futur article 7-2.2 de la loi SRE, quant à lui, n'en contient pas non plus comme il se limite à énoncer que l'injonction mentionne les personnes, les endroits ou encore les moyens de communications ainsi que la nature des données à conserver.

90. Au vu de la jurisprudence de la CJUE, ainsi que des exigences de la CEDH et de la Constitution tel que soulevé aux points 78 et 79 du présent avis, la CNPD estime que la loi devrait prévoir les critères pour délimiter l'étendue de la mesure de conservation.

91. Tel que déjà soulevé, notamment au point 84 du présent avis, il existe une confusion entre la durée de conservation des données et la durée d'application de la mesure. La mesure de conservation ciblée s'étend sur une certaine période pendant laquelle les opérateurs et fournisseurs sont contraints de stocker les données de trafic et de localisation. Une fois cette période venue à échéance, il convient de prévoir la durée pendant laquelle les opérateurs et fournisseurs doivent ensuite conserver les données retenues. La première période correspond à la durée d'application de la mesure, tandis que la deuxième consiste en la durée de conservation proprement dite.

92. La durée de six mois prévue au nouvel article 7-2.3 de la loi SRE semble plutôt être la durée d'application de la mesure. L'article devrait dès lors encore être complété par une durée de conservation.

b. La conservation rapide des données de trafic et de localisation

93. Les exigences de la CJUE quant à l'étendue de la mesure de conservation rapide sont les mêmes qu'à l'égard de la conservation ciblée. La CNPD se limite dès lors à renvoyer à ses observations aux points 88 et suivants du présent avis.

94. En ce qui concerne la durée de conservation, il convient de soulever que, contrairement à la conservation ciblée, il suffit de retenir une seule durée pour cette mesure. En effet, comme il s'agit d'une mesure ponctuelle sur des données déjà générées, il suffit de prévoir pour combien de temps les données doivent être conservées. Néanmoins, il est utile de

relever que la CJUE exige qu'*« afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient »*[224]. La CNPD se voit cependant dans l'impossibilité d'apprécier la proportionnalité de la durée retenue comme les auteurs du projet de loi n'ont pas fourni d'explications à cet égard.

95. Toujours d'après la CJUE, il est nécessaire d'inclure dans la disposition entourant la conservation rapide la finalité pour laquelle cette conservation peut avoir lieu. La CJUE explique à cet égard que *« [d]ans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence »*[225].

96. En effet, la mesure de conservation rapide cible des données qui ont déjà été générées et conservées, par exemple dans un objectif de facturation. Avec la prise d'effet de la mesure, la finalité « conservation pour des motifs de la sauvegarde de la sécurité nationale » s'ajoute à cette finalité initiale. Or, d'après la CJUE, il est nécessaire que la législation nationale prévoie cette nouvelle finalité pour les opérateurs et fournisseurs.
97. Il en est différent de la conservation ciblée qui ne prend effet que pour les données à générer dans le futur et pour lesquelles il existe dès la collecte une double finalité. Les différences non négligeables dans les exigences entourant la conservation ciblée et la conservation rapide la CNPD se pose dès lors la question, s'il ne serait pas utile de séparer les deux mesures.

2. Les mesures de conservation découlant d'une obligation légale

1. Les mesures de conservation du nouvel article 5*bis* de la loi Télécom

98. D'après la compréhension de la CNPD, le nouvel article 5*bis* entend introduire deux mesures de conservation. D'un côté, une conservation ciblée des données de trafic et de localisation délimitée sur base de zones géographiques (a). De l'autre côté, il introduit également une conservation généralisée et indifférencié (b). Comme il ne s'agit pas de

[224] Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 164.
[225] *Ibid.*

ANNEXES

mesures ponctuelles mais d'une obligation de conservation qui incombe aux opérateurs et fournisseurs dans des circonstances spécifiques, cette mesure de conservation ne doit pas être ordonnée mais découle directement de la loi.

a. La mesure de conservation ciblée du nouvel article 5bis de la loi Télécom

99. La mesure de conservation prévue au nouvel article 5*bis*.1 de la loi Télécom est délimitée en fonction de critères géographiques fixés au paragraphe 2 point 1° du même article. Il semble dès lors qu'il s'agit d'une mesure de conservation ciblée.

100. Pour rappel, la CJUE admet la possibilité de prévoir « *aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable* »[226]. Ainsi, la mesure de conservation doit répondre à certains critères énoncés par la CJUE.

101. Il y a lieu de constater que la disposition sous avis respecte les exigences de la CJUE en ce qui concerne la limitation des objectifs pour lesquels une conservation ciblée peut avoir lieu. Comme la disposition se limite néanmoins à mentionner la « criminalité grave » sans définir, par exemple par un seuil tel que retenu au nouvel article 24-3 du CPP, ce qu'il faut entendre par cette notion, la CNPD se demande s'il ne faudrait pas apporter des précisions à cet égard.

102. En ce qui concerne la détermination des catégories de données pouvant être collectées, la CNPD renvoie à ses observations soulevées aux points 53 à 55 du présent avis.

103. Ensuite, elle constate que la limitation de l'étendue se fait sur base de certains des critères géographiques que la CJUE a proposé dans ses arrêts[227]. Ces zones seront définies par le Haut-Commissariat à la protection nationale dans un arrêté grand-ducal sur proposition d'une commission consultative. La CNPD souhaite rappeler l'article 8.2 de la Convention européenne des droits de l'homme, qui prévoit qu' « *[i]l 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 ». De plus, il y a lieu de rappeler que l'article 37 de la Constitution*

[226] Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 168.
[227] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791 et arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258.

exige que « [t]oute limitation de l'exercice des libertés publiques doit être prévue par la loi [...]».

104. Concernant la condition que la mesure doit être nécessaire dans une société démocratique, la CEDH précise que des garanties adéquates et effectives doivent exister afin d'éviter l'arbitraire et les abus. Ainsi la CEDH estime que l'existence d'un contrôle de la nécessité de la mesure est une telle garantie et que l'appréciation doit se faire en prenant en compte toutes les circonstances de l'affaire en question.

105. La CNPD salue dès lors les observations du Conseil d'État formulées à l'encontre de l'arrêté grand-ducal[228], en particulier parce que le commentaire des articles précise que l'étendue du périmètre de chaque zone sera fixée par arrêté grand-ducal qui ne sera pas publié obligatoirement. De plus, comme la commission consultative n'a qu'un rôle de conseil et que son avis n'est pas contraignant pour le Haut-Commissariat à la protection nationale, la CNPD se demande comment le contrôle de la nécessité sera effectué. Sans aucun autre moyen de contrôle effectif, la CNPD considère la publication comme un aspect important dans le cadre du contrôle de la nécessité d'une mesure.

106. En ce qui concerne la revue des zones géographiques, le commentaire des articles indique à juste titre que la CJUE exige que les zones doivent être adaptables notamment lorsque les conditions ayant justifié la conservation changent[229]. La CNPD s'interroge cependant quant à la période de 3 ans retenue pour effectuer cette revue. Les auteurs du projet de loi n'expliquent pas pourquoi ce délai semble approprié de sorte qu'il est impossible d'apprécier ce choix. De plus, la CNPD estime qu'il faudrait prévoir une procédure permettant une revue anticipée au cas où les conditions changent de manière à justifier l'adaptation du périmètre de la zone, voire l'abandon de la surveillance dans une certaine zone.

107. Toujours à l'égard de l'étendue de la mesure, le paragraphe 3 de l'article *5bis* entend introduire l'obligation pour les opérateurs et fournisseurs de continuer de conserver les données de trafic et de localisation des personnes en déplacement, c'est-à-dire des personnes qui au moment d'une communication entrent ou sortent d'une telle zone. La CNPD peut comprendre l'intention des auteurs du projet de loi, mais elle souhaite néanmoins mettre en garde qu'une telle obligation ne doit pas aboutir à une conservation généralisée et indifférenciée sur la quasi-totalité de la population et sur la totalité du territoire. La conservation doit rester l'exception.

108. L'article *5bis*.1 fixe une durée de conservation des données de six mois à partir de la communication. Le commentaire des articles se limite à justifier ce choix par le *« souci d'unification et d'harmonisation des durées de conservation »*. La CNPD est d'avis que cette justification n'est pas suffisante pour apprécier la proportionnalité de la durée retenue.

[228] Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.8.
[229] Voir par exemple arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 82.

ANNEXES

109. De plus, l'article 5*bis* dans sa rédaction actuelle ne contient pas d'indication ou de référence vers la ou les dispositions encadrant l'accès aux données conservées. La CNPD rappelle que l'accès ne peut se faire que dans le respect de la hiérarchie des objectifs. En effet, la CJUE explique que les données conservées pour l'objectif de la sécurité nationale ne peuvent pas être accédées pour des finalités de lutte contre la criminalité grave[230]. L'inverse semble pourtant légitime[231]. Comme l'article sous avis concerne la conservation pour deux objectifs, à savoir la lutte contre la criminalité grave et la préservation de la sécurité nationale, la précision quant aux articles réglant les accès pourrait s'avérer utile. La séparation des mesures en deux articles distincts pourrait également faciliter la compréhension des accès.

b. La mesure de conservation généralisée et indifférenciée du nouvel article 5*bis* de la loi Télécom

110. Le nouvel article 5*bis*.2 point 2° instaure l'obligation pour les opérateurs et fournisseurs de conserver les données de trafic et de localisation de manière généralisée et indifférenciée si *« le niveau de la menace déterminé par le groupe de coordination en matière de lutte contre le terrorisme (GCT) selon l'évaluation visée au plan gouvernemental de vigilance nationale face aux menaces d'actions terroristes (plan „VIGILNAT") est au moins de niveau 3 et couvre l'ensemble du territoire ».*

111. La CNPD tient à rappeler que la conservation généralisée et indifférenciée des données de trafic et de localisation n'est possible que pour des objectifs de la sauvegarde de la sécurité nationale. Or, comme le premier paragraphe de l'article énonce également l'objectif de la lutte contre la criminalité grave, une certaine incertitude quant à la finalité de la conservation généralisée et indifférenciée reste. Même si l'on peut s'imaginer que les conditions qui déclencheraient cette conservation, à savoir que le niveau de la menace soit au niveau 3 au plan VIGILNAT et couvre l'ensemble du territoire, sont en lien avec l'objectif de la sécurité nationale, ceci ne ressort pas clairement du texte. La CNPD se demande dès lors s'il ne serait pas utile de séparer les deux mesures et clarifier qu'une telle conservation généralisée et indifférenciée ne peut se faire que pour l'objectif de la sécurité nationale. Ceci également au vu du respect de la hiérarchie des objectifs expliquée au point 109 du présent avis.

112. Concernant l'étendue de la mesure, et notamment les catégories de données visées, la CNPD n'a pas d'autres observations que celles qu'elle a déjà soulevées aux points 53 à 55 du présent avis, à savoir qu'il doit ressortir clairement de la législation quelles données sont susceptibles d'être collectées.

113. Sans précision quant au moment qui déclenche la durée de la mesure de conservation, la CNPD estime que c'est l'information du Haut-Commissariat à la protection nationale. Le texte ne prévoit

[230] Voir arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702, point 128.
[231] *Ibid.*

pourtant ni une durée de la mesure, ni une procédure pour revoir la nécessité de la mesure ou pour mettre fin à la collecte au cas où elle ne serait plus nécessaire. La CNPD se demande dès lors si le principe de nécessité est respecté à cet égard.

114. Tel que mentionné au point 108 du présent avis, la CNPD se trouve dans l'impossibilité d'apprécier la durée de conservation retenue.

115. Enfin, la CNPD souhaite réitérer ses observations à l'égard de l'utilité d'une référence vers la ou les dispositions encadrant l'accès aux données conservées.

2. La mesure de conservation du nouvel article 10*ter*.1 de la loi Télécom

116. Tel qu'expliqué par le commentaire des articles, la CJUE reconnait la possibilité pour les États membres de prévoir une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques. Ceci notamment parce que *« ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée »*[232]. Il en résulte que l'ingérence dans la vie privée ne peut pas être qualifiée de grave[233].

117. Selon le commentaire des articles, *« compte tenu de la convergence croissante des services de communications électroniques et de l'extension de cette dernière notion, ainsi que de la notion d'opérateur aux acteurs « OTT », à la suite de la transposition du code des communications électroniques européen, il est proposé d'adapter la liste des données d'identification à conserver au-delà des données visées à l'article 10*bis *de la Loi Telecom »*. Ainsi, l'article 10*ter*.1 ne serait qu'un complément de l'article 10*bis*. Si tel est le cas, la CNPD ne comprend pas pourquoi l'article 10bis n'a pas été adapté, d'autant plus que ce dernier contient des références aux articles permettant l'accès aux données conservées.

118. De plus, le point 1° de l'article 10*ter* impose aux opérateurs et fournisseurs de conserver les données qu'ils détiennent au titre de l'article 10*bis*. Est-ce que cette obligation n'est pas superfétatoire du simple fait que les opérateurs et fournisseurs ont déjà cette obligation et qu'un accès à ces données est régi par l'article 10*bis* ? L'interaction entre les deux articles ne semble pas tout à fait claire et prête à confusion.

119. Ensuite, la CNPD s'interroge sur l'utilisation du verbe « générer » dans la partie introductive du paragraphe 1er, ceci notamment en lien avec la collecte des

[232] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 157.
[233] *Ibid.*

ANNEXES

données détenues sur base de l'article 10*bis* ainsi que l'IMEI[234] et l'IMSI[235]. Est-ce que les opérateurs et fournisseurs sont tenus de générer ces données pour leurs abonnés et/ou utilisateurs ? Ou est-ce qu'ils doivent également conserver les données de l'article 10*bis* (nom, prénom, lieu de résidence… etc.), l'IMSI et l'IMEI des destinataires de la communication (par exemple l'appelé) ? Il ne ressort pas clairement du texte que ces données se réfèrent uniquement à l'abonné/l'utilisateur. Au cas où non seulement les données des abonnées/utilisateurs, mais également celles des destinataires de la communication devront être conservées, la CNPD se demande si cette conservation n'irait pas au-delà des limites posées par la CJUE.

120. Par ailleurs, la CNPD constate que certaines notions utilisées dans cet article ne sont pas définies. Il est dès lors incertain ce que l'article vise concrètement. Premièrement, les notions de « données de souscription » et « données d'identification » ne sont pas définies. Il est donc impossible de savoir de quelles données il est question. La notion d'« utilisateur final » n'est pas non plus définie. Est-ce que l'on vise ici la définition retenue dans l'article 2, point 14° de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques ? Enfin, les notions d'« adresses IP ayant servi à la souscription ou à l'activation » ainsi que « le port de source » mériteraient d'être définies afin de savoir quelles données seront collectées concrètement.

121. Vu que la disposition manque de clarté par rapport aux données qui seront traitées, ainsi qu'en ce qui concerne l'interaction avec l'article 10*bis*, la CNPD n'est pas en mesure d'apprécier si les données conservées ne sont pas *« susceptibles de permettre de tirer des conclusions précises, voire très précises, concernant la vie privée des personnes dont les données ont été conservées »*[236] tel que l'exige la CJUE.

3. La mesure de conservation du nouvel article 10*ter*.2 de la loi Télécom

122. D'après la CJUE, *« la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des article 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données »*[237]. La Cour ajoute encore qu'*« [e]u égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation, seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde*

[234] Selon le commentaire des articles, l'IMEI *« est un numéro d'identification unique qui permet d'immatriculer un équipement mobile ».*
[235] Selon le commentaire des articles, l'IMSI *« est un identifiant qui se trouve dans la carte SIM et qui permet d'identifier de manière unique chaque abonné ».*
[236] Voir arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788, point 60.
[237] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 155.

de la sécurité nationale, à justifier cette ingérence »[238].

123. Il y a lieu de constater que la disposition sous avis semble respecter les exigences de la CJUE en ce qui concerne la limitation des objectifs pour lesquels une conservation ciblée peut avoir lieu. Comme la disposition se limite néanmoins à mentionner la « criminalité grave » sans définir, par exemple par un seuil tel que retenu au nouvel article 24-3 du CPP, ce qu'il faut entendre par cette notion, la CNPD se demande s'il ne faudrait pas apporter des précisions à cet égard.

124. À cet égard, il faut prendre en compte la récente jurisprudence de la CJUE qui n'existait pas encore au moment du dépôt du projet de loi sous avis. Il s'agit de l'arrêt du 30 avril 2024. La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), qui contient des observations[239] quant à la possibilité de prévoir une conservation généralisée et indifférenciée des adresses IP attribuées à la source aux fins d'objectifs de lutte contre les infractions pénales en général.

125. La Cour apporte des précisions à sa position soulevée au point 122 du présent avis, et explique qu'elle *« s'est expressément fondée, pour parvenir à cette conclusion, sur le caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7, 8 et 11 de la Charte qu'est susceptible de comporter une telle conservation des adresses IP »*[240]. Elle ajoute que l'ingérence grave dérive du fait qu'il est possible d'effectuer un traçage exhaustif du parcours de navigation de la personne concernée ou d'établir le profil détaillé. D'après la Cour un tel profilage ou traçage n'est possible que si les différentes informations conservées, dont les adresses IP, sont combinées. Grâce à cette combinaison, il est dès lors possible de tirer des conclusions précises sur la vie privée des personnes concernées[241].

126. Il apparaît donc que ce n'est pas nécessairement la conservation généralisée et indifférenciée des adresses IP attribuées à la source qui constitue une ingérence grave dans la vie privée des personnes concernées, mais plutôt la possibilité de combiner ces données avec d'autres données collectées. La CJUE précise dès lors que *« l'obligation faite aux fournisseurs de services de communications électroniques, par une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002/58, d'assurer la conservation généralisée et indifférenciée des adresses IP peut, le cas échéant, être justifiée par l'objectif de la lutte contre les infractions pénales en général lorsqu'il est effectivement exclu que cette conservation puisse engendrer des ingérences graves dans la vie privée de la personne concernée en raison de la possibilité de tirer des conclusions précises sur celle-ci moyennant, notamment, une mise en relation de ces adresses IP avec*

[238] *Ibid*, point 156.
[239] Voir arrêt du 30 avril 2024, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370, points 66 à 94.
[240] *Ibid*., point 77.
[241] *Ibid*., points 78 à 80.

ANNEXES

un ensemble de données de trafic ou de localisation qui auraient également été conservées par ces fournisseurs »[242].

127. La Cour en déduit qu'un *« Étant membre qui entend imposer aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des adresses IP en vue d'atteindre un objectif lié à la lutte contre les infractions pénales en général doit s'assurer que les modalités de conservation de ces données soient de nature à garantir qu'est exclue toute combinaison desdites adresses IP avec d'autres données conservées, dans le respect de la directive 2002/58, qui permettrait de tirer des conclusions précises sur la vie privée des personnes dont les données seraient ainsi conservées »*[243].

128. La Cour exige en effet une séparation stricte entre les différentes catégories de données conservées. Cette exigence fait penser à l'image de plusieurs coffres-forts qui contiennent les différentes catégories de données et qui empêchent que les données puissent être reliées entre eux. La Cour ajoute encore que la législation nationale doit prévoir *« des règles claires et précises relatives auxdites modalités de conservation, ces modalités devant répondre à des exigences strictes »*[244].

129. Aux points 86 à 89, la CJUE fournie des précisions quant à ces modalités. Il faut ainsi que les données soient conservées séparément, et que sur un plan technique cette séparation soit étanche. Une troisième exigence de la Cour consiste en la mise en place d'un procédé technique performant qui effectue la mise en relation entre les adresses IP et les données d'identité civile conservée, ceci dans un objectif de préserver la séparation étanche. En dernier lieu, la CJUE exige que la séparation étanche fasse l'objet d'un contrôle régulier par une autorité publique. La CJUE conclut que lorsque ces modalités sont respectées et qu'il n'est pas possible de combiner des données pour tirer des conclusions précises sur la vie privées des personnes concernées, une conservation généralisée et indifférenciée des adresses IP aux fins d'un objectif de lutte contre les infractions pénales en général est possible.

130. Au vu de ce qui précède, la CNPD estime que la disposition sous examen devrait être revue pour respecter la récente jurisprudence de la CJUE.

131. De plus, faute de fournir des explications dans le commentaire des articles quant au choix de la durée de conservation retenue, la CNPD se trouve dans l'impossibilité de l'apprécier.

132. Enfin, il y a lieu de soulever que le terme « port » utilisé à la fin du premier alinéa prête à confusion. De quoi s'agit-il exactement ? Est-ce qu'il s'agit des mêmes « ports source de la connexion » mentionnés au paragraphe 1er ? Dans l'affirmative, ne faudrait-il pas aligner la terminologie ?

[242] *Ibid.*, point 82.
[243] *Ibid.*, point 83.
[244] *Ibid.*, point 85.

3. Les garanties entourant la conservation par les opérateurs et fournisseurs

133. Bien que les mesures de conservation doivent être accompagnées de garanties en ce qui concerne la possibilité d'y avoir recours, la CJUE exige également que la conservation en elle-même par les opérateurs et fournisseurs soit entourée de garanties contre les risques d'abus et d'accès illicites.

134. La CJUE explique en effet que *« compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée et indifférenciée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite »*[245].

135. Ainsi, la Cour exige notamment que les opérateurs et fournisseurs détruisent de manière irrémédiable les données à la fin de la durée de conservation[246], qu'ils conservent les données sur le territoire de l'Union[247], qu'ils assurent la pleine intégrité et la confidentialité desdites données et garantissent un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles appropriées. Par ailleurs, elle exige que les États membres garantissent un contrôle, par une autorité indépendante, du respect du niveau de protection garanti par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel[248].

136. En l'occurrence, c'est l'article 2 points 3° et 8° du projet de loi qui est intéressant à cet égard comme il modifie les articles 5 et 9 de la loi Télécom.

137. Concernant la destruction irrémédiable préconisée par la CJUE, la CNPD constate que tant la version modifiée de l'article 5 que celle de l'article 9 de la loi Télécom prévoient que les données de trafic et de localisation sont supprimées ou rendues anonymes *« dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication »*. Il existe des exceptions à cette suppression, notamment à l'article 5.2 et 5.3 de la loi Télécom, qui semblent admissibles et ne soulèvent pas d'observations particulières de la part de la CNPD. Cependant, les articles 5.1 et 9.1 de la loi Télécom prévoient une autre exception qui, a priori, semble logique mais qui mériterait néanmoins d'être précisée.

138. En effet, l'article 9.1 prévoit que les données de trafic et de localisation sont supprimées lorsqu'elles ne sont plus nécessaires à la transmission d'une communication *« à l'exception des accès qui sont ordonnés par les autorités judiciaires et par le comité ministériel du renseignement pour le Service de renseignement de l'État*

[245] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 119.
[246] Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 67.
[247] *Ibid.*, point 68.
[248] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 123.

ANNEXES

agissant dans le cadre des compétences leur attribuées par la loi pour sauvegarder la sécurité nationale, pour la lutte contre la criminalité grave et pour la prévention de menaces graves contre la sécurité publique ». La rédaction de l'article 5.1 est similaire.

139. La CNPD se demande si cette partie de la phrase doit être comprise comme la conséquence logique de la possibilité pour certaines autorités de demander la conservation des données aux opérateurs et fournisseurs. En d'autres termes, est-ce qu'il s'agit d'une simple confirmation du principe que des mesures de conservation peuvent être mises en place ? Si tel est le cas, il convient néanmoins de s'interroger sur les termes utilisés. Il n'est effectivement pas clair pourquoi l'article dispose que *« [...] à l'exception des accès qui sont ordonnés par les autorités judiciaires et par le comité ministériel du renseignement [...] »*. Ne devrait-on pas plutôt écrire « à l'exception des données dont la conservation a été ordonnée [...] » ?

140. La rédaction actuelle laisse effectivement un doute quant à la suppression des données dont la conservation a été ordonnée, enjointe ou prévue par un texte légal, et qui par la suite ont été accédées par les autorités compétentes. Si la lecture de l'article devait être telle que les données qui ont été accédées ne seront pas supprimées, ceci serait contraire à la jurisprudence de la CJUE.

141. De plus, la CNPD considère qu'il faudrait prévoir une durée de conservation maximale de ces données. Ceci notamment par rapport à ce qui a été soulevé dans le présent avis pour plusieurs mesures de conservation, à savoir qu'il ne ressort pas clairement des dispositions pendant combien de temps les données doivent être conservées par les opérateurs et fournisseurs comme il y a un mélange entre durée d'application de la mesure et durée de conservation des données[249].

142. Concernant la limitation des accès aux personnes strictement nécessaires, les futurs articles 5.4 et 9.4 de la loi Télécom semblent refléter cette exigence de la CJUE. Un contrôle par une autorité indépendante compétente en matière de protection des données est également prévu.

143. Il convient néanmoins de se demander pourquoi les auteurs du projet de loi n'ont pas inclus les autres exigences de la CJUE à savoir que les opérateurs et fournisseurs doivent conserver les données sur le territoire de l'Union et assurer la pleine intégrité et la confidentialité desdites données, et garantir un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles appropriées.

144. En dernier lieu, il faut constater qu'aucune mesure de conservation ne contient des garanties envers les personnes soumises au secret professionnel au sens de l'article 458 du Code pénal ainsi que les lanceurs d'alerte. La CJUE explique en effet que *« la conservation des données relatives au trafic et des données de localisation à des*

[249] Voir par exemple points 58 et 59 du présent avis.

fins policières est susceptible, à elle seule, de porter atteinte au droit au respect des communications [...] et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de [la Charte]. Or, de tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte [...]. En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés »[250]. La CNPD regrette dès lors que les auteurs du projet de loi n'aient pas prévu des garanties à l'égard de ces catégories de personnes.

XX. Les mesures législatives d'accès aux données

145. Une fois les données conservées, il est nécessaire de prévoir un deuxième ensemble de mesures autorisant les autorités compétentes à accéder les informations. La CJUE explique clairement qu'elle considère que l'accès par les autorités compétentes aux données conservées constitue une ingérence supplémentaire dans la vie privée des personnes concernées[251].

146. Ainsi, et comme les mesures d'accès correspondent, tout comme les mesures de conservations, à une dérogation au principe de confidentialité, elles doivent également respecter les exigences de la CJUE[252].

147. Les mesures d'accès doivent dès lors « être subordonnées à des garanties appropriées »[253] et ainsi « prévoir des règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données. De même, une mesure de cette nature doit être légalement contraignante en droit interne »[254]. La Cour ajoute encore qu'« une telle réglementation nationale doit également prévoir les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées »[255].

148. La jurisprudence de la Cour fournit des indications sur ce qu'une mesure législative d'accès doit contenir. Elle exige par exemple que la législation contienne des critères afin de limiter le nombre de personnes ayant accès aux données[256]. Elle considère par ailleurs *« qu'un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire »*[257]. Il est dès lors essentiel que

[250] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 118.
[251] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 116 et arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788, point 51.
[252] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 165.
[253] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 117.
[254] *Ibid.*
[255] *Ibid.*, point 118.
[256] Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 62.
[257] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.

ANNEXES

la loi contienne *« des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des abonnés ou des utilisateurs inscrits. À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction [...].»*[258].

149. Ainsi, outre l'exigence que seulement les personnes strictement nécessaires aient accès aux données, la Cour exige que la loi fixe des critères et conditions déterminant dans quels cas les données peuvent être accédées. De plus, la CJUE demande qu'il existe un lien au moins indirect entre l'objectif de lutte contre la criminalité et la personne dont les données seront accédées. Pour cette dernière exigence, la Cour admet néanmoins une atténuation en cas de menace par des activités terroristes. Dans ce cas, il suffit que des éléments objectifs permettent de démontrer que les informations accédées puissent contribuer à la lutte contre de telles activités[259].

150. En ce qui concerne les objectifs des mesures d'accès, la jurisprudence de la CJUE répète à plusieurs reprises que dans le respect de la hiérarchie des objectifs, l'accès aux données *« ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il n'en va autrement que si l'importance de l'objectif poursuivi par l'accès dépasse celle de l'objectif ayant justifié la conservation »*[260]. Ainsi, quand des données ont été conservées pour des objectifs de sauvegarde de la sécurité nationale, elles ne peuvent pas être accédées pour des objectifs de lutte contre la criminalité grave. L'inverse serait cependant admissible.

151. D'un point de vue procédural, la CJUE exige que la mesure d'accès fasse l'objet d'un *« contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales »*[261].

152. La CJUE n'admet le contrôle postérieur qu'en cas d'urgence dûment justifiée. Le contrôle doit alors intervenir dans les plus brefs délais[262]. La Cour explique à cet égard qu'un *« contrôle ultérieur ne permettrait pas de répondre à l'objectif d'un contrôle préalable, consistant à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire »*[263].

[258] *Ibid.*
[259] *Ibid.*
[260] Voir arrêt du 20 septembre 2022 SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702, point 128.
[261] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 120.
[262] Voir arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 58.
[263] *Ibid.*

153. Une garantie supplémentaire contre les risques d'abus que la CJUE juge importante est « *que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités* »[264]. Ainsi, les mesures législatives doivent prévoir une telle information des personnes concernées qui est effectivement nécessaire pour leur permettre d'exercer leurs droits en matière de protection des données.

154. Enfin, la CJUE soulève que la transmission par les opérateurs et fournisseurs de données de trafic et de localisation aux autorités répressives entraine des « *effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de la Charte. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte* »[265]. Il serait dès lors souhaitable qu'une mesure législative d'accès prévoit des garanties à l'égard des personnes soumises au secret professionnelles ainsi que des lanceurs d'alerte.

155. À la lecture du projet de loi, il devient clair qu'il existe quatre mesures législatives qui régissent les accès aux données conservées. Trois de ces mesures sont prévues dans le Code de procédure pénale, notamment aux articles 48-27 du CPP (1) et l'article 67-1 du CPP (2) et une est prévue par l'article 7.2 de la loi SRE (3). Il convient dès lors de voir si les différentes mesures d'accès respectent les exigences de la CJUE décrites ci-avant.

1. Les mesures d'accès sur base de l'article 48-27 du Code de procédure pénale

156. L'article 1er point 2° du projet de loi entend remplacer l'article 48-27 du CPP et ajoute une nouvelle mesure d'accès à la mesure d'accès aux données d'identification (1) déjà prévue à cet article. En effet, le nouveau paragraphe 2 de l'article 48-27 du CPP introduit une mesure d'accès relative aux données IP (2). Comme ces deux mesures doivent répondre à des exigences différentes, il est nécessaire de les examiner séparément.

1. La mesure d'accès aux données d'identification sur base de l'article 48-27.1 du Code de procédure pénale

157. Le projet de loi entend adapter la rédaction de l'article 48-27 du CPP pour refléter les changements de la loi Télécom, notamment l'introduction de l'article 10*ter*.1 qui prévoit l'obligation légale pour les opérateurs et fournisseurs de conserver les données d'identification des utilisateurs. Ainsi, l'article 48-27.1 du CPP dans sa rédaction nouvelle attribuera la possibilité au juge d'instruction et au procureur d'État d'accéder à ces données d'identification.

[264] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 190.
[265] Voir arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 72.

ANNEXES

158. En ce qui concerne les objectifs pour lesquels un accès aux données conservées est possible, il y a lieu de constater que la disposition sous avis ne limite pas l'applicabilité à des infractions spécifiques. Ainsi, le recours à cette mesure d'accès est possible tant pour la sauvegarde de la sécurité nationale que pour la lutte contre la criminalité grave ainsi que pour la lutte contre la criminalité en général.

159. Dans l'arrêt Ministerio Fiscal de 2018[266], la CJUE a pu se prononcer sur une telle mesure d'accès aux seules données d'identification. Elle clarifie en particulier la question de savoir pour quels objectifs (sécurité nationale, criminalité grave, criminalité simple) un accès aux seules données d'identification est possible.

160. Il ressort clairement de cet arrêt que la Cour détermine la gravité de l'ingérence dans la vie privée des personnes concernées en fonction de la nature des données accédées. Ainsi, lorsque sont accédées des données qui ne permettent pas de tirer des conclusions précises concernant la vie privée des personnes concernées, l'ingérence n'est pas qualifiée de grave. Dans le cas concret de l'arrêt Ministerio Fiscal, les données permettaient *« uniquement de mettre en relation, pendant une période déterminée [12 jours], la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée »*. La Cour conclut par dire que si l'accès vise donc des données d'identité civile, c'est-à-dire le nom, prénom, et le cas échéant l'adresse, ainsi que les seuls numéros de téléphone correspondant à ces cartes SIM, cette ingérence ne peut pas être qualifiée de grave.

161. Dans le même arrêt, la CJUE soulève que *« lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général »*. Il en résulte que, pour autant qu'elles ne permettent pas de tirer de conclusions précises concernant la vie privée des personnes concernées, l'accès aux données permettant l'identification des utilisateurs est possible pour les objectifs de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave ainsi que de lutte contre la criminalité en général.

162. Au vu de ce qui précède, la disposition sous avis semble en conformité avec la jurisprudence de la CJUE, mais uniquement dans la mesure où elle ne vise effectivement que l'accès aux données aux fins d'identification des utilisateurs. Vu la rédaction actuelle de l'article, la CNPD se pose plusieurs questions.

[266] Voir arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788, points 48 à 63.

163. Premièrement, il convient de s'interroger sur la partie de phrase *« sur la base de toutes données détenues par lui sur base de l'article 10*ter*, paragraphe 1er, de la loi modifiée du 30 mai 2005 »* du 1er paragraphe de l'article 48-27 du CPP. Au vu de ce qui a été soulevé dans la partie I.B.2 et en particulier au point 119 du présent avis, la CNPD se demande si on ne vise réellement que des données d'identification ou si cela va au-delà. Dans ce dernier cas, la disposition ne serait pas conforme à la jurisprudence de la CJUE.

164. Deuxièmement, la CNPD émet également des doutes quant à l'étendue du point 2° du paragraphe 1er en ce qu'il prévoit un accès à des fins d'*« identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée »*. Est-ce qu'une telle identification des services utilisés n'irait pas au-delà de ce qui est autorisé par la CJUE qui fait explicitement référence à la possibilité d'accéder aux données à des fins d'identification des utilisateurs ?

165. Si l'accès visé à l'article 48-27.1 du CPP serait plus large et qu'il viserait également des données qui doivent être considérées comme des données de trafic et de localisation, alors l'accès devrait être considéré comme permettant de tirer des conclusions précises concernant la vie privée des personnes concernées. L'ingérence devrait dès lors être qualifiée de grave et un accès ne pourrait être possible que pour les objectifs de préservation de la sécurité nationale et de lutte contre la criminalité grave.

166. Ensuite, en ce qui concerne l'exigence de la CJUE qu'*« un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction »*[267], la CNPD constate que le projet de loi ne la prévoit pas expressément. Elle estime qu'il appartient au juge d'instruction ou au procureur d'État de justifier l'existence d'un tel lien entre la personnes concernée et l'objectif poursuivi dans la décision motivée et écrite mentionnée dans l'article 48-27.1 du CPP. La CNPD se demande néanmoins s'il ne faudrait pas modifier le texte à cet égard.

167. Par ailleurs, il y a lieu de constater que la mesure d'accès aux données d'identité civile ne contient pas la garantie de l'information des personnes concernées par les autorités compétentes que leurs données ont été accédées. Dans la mesure où la CJUE exige l'existence d'une telle garantie, la CNPD estime que la disposition devrait être complétée.

168. Enfin, la CNPD regrette que l'article 48-27 du CPP ne contienne pas de garanties à l'égard des personnes soumises au secret professionnel ainsi que les lanceurs d'alerte.

2. La mesure d'accès aux données d'identification sur base de l'article 48-27.2 du Code de procédure pénale

169. Ensuite, le projet de loi entend introduire une nouvelle mesure d'accès à l'article 48-27.2 du CPP, à savoir la possibilité

[267] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.

ANNEXES

d'accéder, sur décision du procureur d'État ou du juge d'instruction et à des fins d'identification de l'utilisateur, aux données IP conservées au titre du nouvel article 10*ter*.2 de la loi Télécom.

170. Il convient de rappeler que la jurisprudence récente de la CJUE doit être prise en considération pour cette mesure, à savoir l'arrêt du 30 avril 2024, précité La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon) en particulier les points 95 à 122. Cet arrêt apporte des précisions, par rapport aux exigences auxquelles une disposition législative prévoyant l'accès aux adresses IP conservées doit répondre, y compris en ce qui concerne le contrôle préalable.

171. En ce qui concerne les exigences auxquelles une mesure d'accès aux adresses IP attribuées à la source doit répondre, et spécifiquement les objectifs pour lesquelles un tel accès peut être décidé, la Cour opère un lien avec ses observations sur la conservation de telles données. Ainsi, la Cour estime que la conservation séparée et étanche des données constitue le prérequis pour que l'accès aux adresses IP attribuées à la source pour des infractions dites simples soit possible. Ceci notamment pour garantir que l'ingérence dans la vie privée des personnes reste la moins intrusive possible dans la mesure où aucun traçage ou profilage ne soit possible du fait que les données puissent être combinées.

172. En revanche, la Cour indique que seule la finalité de l'identification justifierait un accès aux adresses IP dans le cadre de la lutte contre la criminalité dite simple et que la mesure législative doit contenir des garanties contre des abus. Elle ajoute encore, qu'il faut toujours respecter le principe de la hiérarchie des objectifs.

173. La CNPD considère en conséquence que la disposition sous examen doit être revue afin de respecter cette jurisprudence. Elle se félicite par ailleurs que la mesure ne peut être prise qu'aux seules fins d'identification. En effet, toute utilisation à d'autres fins semble non-conforme à la jurisprudence de la CJUE.

174. Néanmoins, en ce qui concerne l'exigence de la CJUE qu'*« un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction »*[268], la CNPD constate que le projet de loi ne la prévoit pas expressément. Elle renvoie à cet égard à ces observations soulevées au point 166 du présent avis.

175. La CNPD se demande encore pourquoi cette mesure est régie par l'article 48-27 du CPP et non pas par l'article 67-1 du CPP, notamment au regard de l'exigence de la CJUE de la nécessité d'un contrôle indépendant préalable pour l'accès à des données de trafic ou de localisation.

176. En effet, la CJUE explique qu'*« il est essentiel que l'accès des autorités nationales compétentes aux données conservées*

[268] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.

soit subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales »[269]. Elle poursuit en soulevant que *« l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable [...] impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure »*[270]. La Cour soutient encore que *« [t]el n'est pas le cas d'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique »*[271] et conclut que *« le ministère public n'est pas en mesure d'effectuer le contrôle préalable »*[272].

177. D'après la compréhension de la CNPD, le procureur d'État ne devrait dès lors pas être en mesure d'enjoindre une telle mesure d'accès. Cette possibilité ne devrait être attribuée qu'au seul juge d'instruction.

178. De plus, il convient de souligner que la CJUE admet la possibilité d'accéder aux données de trafic et de localisation sans autorisation préalable mais ce uniquement en cas d'urgence dûment justifiée. Dans cette situation, le contrôle doit néanmoins intervenir dans des brefs délais. Une telle procédure d'urgence est prévue à l'article 48-27.3 du CPP. La CNPD constate néanmoins que la disposition ne contient pas de délai endéans duquel le contrôle doit être effectué. Elle se demande s'il ne faudrait pas prévoir un délai maximal suffisamment court pour être conforme à la jurisprudence de la CJUE.

179. Encore faut-il soulevé que la jurisprudence récente de la CJUE admet une atténuation à cette position[273]. En effet, en admettant la conservation et l'accès des adresses IP attribuées à la source dans le cadre de la lutte contre la criminalité dite simple à des fins d'identification, la Cour ne manque pas de se prononcer sur le contrôle préalable par une juridiction ou une autorité administrative indépendante dans ce contexte. Ainsi, la Cour souligne que *« dans le cas où un dispositif de conservation tel que celui décrit aux points 86 à 89 du présent arrêt est mis en place, l'accès de l'autorité publique aux données relatives à l'identité civile correspondant aux adresses IP ainsi conservées n'est, en principe, pas subordonné à l'exigence d'un contrôle préalable par une juridiction ou par une entité administrative indépendante »*[274]. Il convient donc également de revoir, le cas échéant, la disposition sous examen, afin de respecter les observations de la CJUE.

[269] Voir arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 51.
[270] *Ibid.*, point 54.
[271] *Ibid.*, point 57.
[272] *Ibid.*
[273] Voir arrêt du 30 avril 2024, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370, en particulier les points 123 à 151.
[274] *Ibid.*, point 134.

ANNEXES

180. Concernant la garantie des personnes concernées d'être informées de l'accès à leurs données à caractère personnel, la CNPD renvoie à ses observations soulevées au point 167 du présent avis.

181. Enfin, la CNPD regrette que l'article 48-27 du CPP ne contienne pas de garanties à l'égard des personnes soumises au secret professionnel ainsi que les lanceurs d'alerte.

2. La mesure d'accès sur base de l'article 67-1 du Code de procédure pénale

182. Selon le commentaire des articles, l'article 67-1 du CPP dans sa rédaction nouvelle *« vise l'accès des autorités judiciaires aux données relatives au trafic et de localisation, conservées par les opérateurs et fournisseurs concernés conformément aux dispositions inscrites à la Loi Telecom ainsi que désormais au titre du nouvel article 24-3 du Code de procédure pénale proposé par le présent projet de loi »*.

183. Ainsi, l'intention des auteurs du projet de loi semble être que le juge d'instruction peut ordonner non seulement l'accès aux données conservées pour des motifs de lutte contre la criminalité grave, mais également pour les besoins de sauvegarde de la sécurité nationale au titre de l'article 5bis de la loi Télécom.

184. Elle note néanmoins que l'article 67-1 du CPP ne semble viser que les situations où *« les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ».*

185. À cet égard, la CNPD souhaite rappeler que conformément au principe de la hiérarchie des objectifs, l'accès aux données conservées *« ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il n'en va autrement que si l'importance de l'objectif poursuivi par l'accès dépasse celle de l'objectif ayant justifié la conservation »*[275]. Il en résulte que des données conservées, par exemple pour des motifs de sauvegarde de la sécurité nationale, ne peuvent pas être accédées pour des objectifs de lutte contre la criminalité grave.

186. La CNPD est consciente du fait que la terminologie *« les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement »* semble a priori également comprendre les infractions qui mettent en péril la sécurité nationale. Il convient néanmoins de s'interroger comment, en pratique, la distinction entre un accès aux données conservées pour des motifs de lutte contre la criminalité grave et un accès aux données conservées pour les besoins de sauvegarde de la sécurité nationale s'opère.

187. Ou bien faut-il lire l'article 67-1 du CPP de manière à ce que le juge ne puisse pas ordonner un accès aux données conservées pour les besoins de sauvegarde de la sécurité nationale ? Dans ce cas, ne priverait-on pas le juge d'instruction d'une mesure nécessaire dans le cadre de l'instruction ?

[275] Voir arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 98.

188. Est-ce que la rédaction de l'article 67-1 du CPP ne devrait pas être revue afin de s'assurer que le juge d'instruction ait toutes les mesures d'accès nécessaires à sa disposition, tout en respectant le principe de la hiérarchie des objectifs ?

189. En ce qui concerne les critères objectifs pour définir les circonstances et les conditions dans lesquelles les autorités nationales compétentes peuvent obtenir accès aux données conservées, les auteurs du projet de loi indiquent dans le commentaire des articles que *« l'article 67-1 soumet d'ores et déjà l'accès aux données conservées à la condition préalable de faits qui* « emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement » ». Selon les auteurs du projet de loi, cette condition semble suffisante pour répondre aux exigences de la CJUE.

190. La CNPD se demande pourtant si la disposition sous avis répond avec suffisance à l'exigence qu'il existe un *« lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire »*[276]. La CJUE exige que la législation prévoie l'existence d'un lien au moins indirect entre l'objectif de lutte contre la criminalité et la personne dont les données seront accédées. Pour cette dernière exigence, la Cour admet néanmoins une atténuation en cas de menace par des activités terroristes. Dans ce cas il suffit que des éléments objectifs permettent de démontrer que les informations accédées puissent contribuer à la lutte contre de telles activités[277]. Elle renvoie à cet égard à ses observations soulevées au point 166 du présent avis.

191. Par ailleurs, concernant l'exigence *« que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités »*[278], la CNPD se félicite que le projet de loi conserve cette garantie supplémentaire contre les risques d'abus.

192. La CNPD se demande néanmoins comment cette garantie est mise en œuvre dans la pratique. Comment les personnes qui, in fine, ne font pas l'objet d'une procédure pénale sont informées ? Est-ce que toutes les personnes sont informées, à savoir la personne ciblée ainsi que les personnes avec lesquelles cette dernière était en correspondance ?

193. Enfin, la CNPD regrette que l'article 67-1 du CPP ne contienne pas de garanties à l'égard des personnes soumises au secret professionnel ainsi que les lanceurs d'alerte.

3. La mesure d'accès sur base de l'article 7.2 de la loi SRE

194. Bien que le projet de loi n'entende apporter que des modifications mineures

[276] Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.
[277] *Ibid.*
[278] Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 190.

ANNEXES

à l'article 7 de la loi SRE, la CNPD estime nécessaire de soulever quelques observations étant donné qu'il régit l'accès du SRE à des données de trafic et de localisation.

195. Ainsi, la CNPD se pose notamment la question si l'article 7 de la loi SRE régit également l'accès de ce dernier aux données d'identification conservées au titre de l'article 10*ter* de la loi Télécom. La partie de phrase *« y compris l'identification des correspondants et de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications »* semble indiquer que tel est le cas. La CNPD estime néanmoins que des précisions, par exemple sous forme de renvoi, pourraient servir à la lisibilité et à la compréhension de la mesure d'accès.

196. Ensuite, il y a lieu de constater que la mesure d'accès aux données ne contient pas la garantie de l'information des personnes concernées par les autorités compétentes que leurs données ont été accédées. Dans la mesure où la CJUE exige l'existence d'une telle garantie, la CNPD se demande s'il ne faudrait pas compléter l'article 7 de la loi SRE.

197. Enfin, la CNPD se félicite que les auteurs du projet de loi ont maintenu dans l'article 7.3 alinéa 5 une garantie pour les données de *« personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes elles-mêmes d'être impliquées dans une menace actuelle ou potentielle relevant du champ d'application des missions du SRE déterminés à l'article 3 »*[279]. En effet, cette garantie répond au moins en partie aux risques exprimés par la CJUE que la transmission par les opérateurs et fournisseurs de données de trafic et de localisation aux autorités répressives entraine des *« effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de la Charte. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte »*[280].

XXI. Les autres dispositions modificatives

4. L'alignement de la définition du consentement à celle retenue par le RGPD

198. L'article 2 point 1° du projet de loi vise selon le commentaire des articles à aligner la définition du terme « consentement » de la loi Télécom à celle utilisée dans le RGPD. La CNPD constate néanmoins qu'il ne s'agit pas d'une reprise fidèle de la définition et s'interroge sur cette adaptation.

5. Les modifications apportées à l'article 5-1 de la loi Télécom (désormais article 5ter de la loi Télécom)

199. La CNPD s'interroge sur la plus-value du paragraphe 1er. En effet, la disposition prévoit que *« [l]es données conservées au titre des articles 5, 5bis et 9 de la présente loi par les autorités compétentes au sens de l'article 1er, paragraphe 1er, de la loi du 1er août*

[279] Loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État, article 7 paragraphe 3 alinéa 5.
[280] Voir arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 72.

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 sont soumises aux exigences prévues à l'article 28 de cette même loi ». Dans la mesure où la loi précitée du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale s'applique de toute manière aux traitements effectués par ces autorités pour autant que le traitement ait lieu à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, la CNPD ne comprend pas la raison d'être de cette disposition.

200. De plus, il convient de s'interroger sur la rédaction du paragraphe 2 en ce qu'il prévoit que *« [l]es données sont détruites lorsque la durée de conservation prend fin, à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées »*. Est-ce que cette disposition s'applique aux autorités compétentes, c'est-à-dire aux autorités qui ont accédé ou auxquelles les données ont été transmises, ou est-ce qu'elle s'applique aux opérateurs et fournisseurs ? Il convient encore de se demander comment cette disposition interagit avec les autres dispositions contenant des durées de conservation. Enfin, la partie de phrase *« à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées »* suscite des interrogations de la part de la CNPD, étant donné que cette exception semble impliquer que certaines données n'ont pas de durée de conservation maximale. La CNPD estime dès lors que ce paragraphe mérite d'être clarifié.

XXII. Observations supplémentaires

201. La CNPD saisit l'occasion du projet de loi de soulever que pour des violations en matière de protection des données de la loi Télécom elle n'est actuellement pas en mesure de recourir à ses pouvoirs découlant de l'article 58 du RGPD. Elle suggère dès lors fortement au législateur de prévoir une disposition afin d'étendre les compétences et pouvoirs de la CNPD à l'égard de la loi Télécom. Ainsi, elle propose, par exemple, de compléter l'article 12 de la loi Télécom par un deuxième paragraphe avec une teneur similaire de l'article 12 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 :

> *« (2) Dans le cadre des missions conférées par le paragraphe 1er, la CNPD dispose des pouvoirs prévus à l'article 58 du règlement (UE) 2016/679. »*

202. De plus, la CNPD souhaite soulever que deux dispositions de la loi Télécom ne semblent plus en adéquation avec la législation actuelle concernant la protection des données, étant donné que le RGPD est entré en application en 2018 et que la loi Télécom date de 2005. Il s'agit d'un côté des paragraphes 3 à 5 de l'article 3 de la loi Télécom qui traitent des violations de données à caractère personnel, et plus particulièrement des notifications à faire à la CNPD, de l'inventaire à tenir ainsi que de la sanction pénale en cas de manquement aux obligations. Le RGPD connaît un régime spécifique pour les violations des données à

ANNEXES

caractère personnel qui diffère dans certains points à celui prévu par la loi Télécom. Ainsi, le régime du RGPD ne connaît pas, par exemple, de sanction pénale. De plus, la CNPD ne comprend pas ce qui justifie que le régime des notifications de violations de la loi Télécom reste différent de celui prévu par le RGPD, notamment par rapport aux acteurs du terrain qui doivent se conformer à ces deux régimes. Elle suggère dès lors d'd'aligner la loi Télécom à ce qui est prévu par le RGPD en remplaçant les trois paragraphes par une référence aux dispositions pertinentes du RGPD.

203. De l'autre côté, il s'agit de l'article 4(3)(e) de la loi Télécom qui prévoit une dérogation au principe de confidentialité lorsque l'abonné ou l'utilisateur a donné son consentement. Il importe de soulever que le RGPD a défini le consentement comme *« toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »*. Les termes importants de cette définition sont *« par une déclaration ou par un acte positif clair »*. Il faut dès lors que la personne concernée ait donné son consentement de manière explicite. Le recueil implicite du consentement n'est plus valable[281]. Or, la rédaction actuelle de l'article 4(3)(e) et en particulier la dernière phrase de ce point[282] rend possible le recueille implicite du consentement.

204. Il importe de soulever qu'il ressort de la guidance du Comité européen pour la protection des données que l'article 95 du RGPD implique qu' *« [a]ussi les conditions d'obtention d'un consentement valable établies par le RGPD sont-elles applicables dans les situations tombant dans le champ d'application de la directive* «vie privée et communications électroniques» »[283]. La CNPD note encore que la volonté des auteurs du projet de loi d'aligner la définition de consentement dans la loi Télécom avec celle du RGPD démontre que ce terme doit être compris de la même manière. La CNPD estime donc essentiel que cette dernière phrase de l'article 4(3)(e) de la loi Télécom soit supprimée.

Ainsi adopté à Belvaux
en date du 16 mai 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[281] Ainsi, par exemple, un site ne peut plus afficher des cases déjà cochées pour recueillir le consentement. Il faut que la personne concernée coche la case lui-même.
[282] Article 4(3)(e) dernière phrase de la loi Télécom : « Lorsque cela est techniquement possible et effectif, l'accord de l'abonné ou de l'utilisateur peut être exprimé par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application ».
[283] Voir les lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/769 du comité européen pour la protection des données, point 7.

6

Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°7961 modifiant 1° la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises ; 2° la loi modifiée du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs

Délibération n°29/AV13/2024
du 16 mai 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Le 31 mars 2023, la CNPD a avisé le projet de loi n°7961 modifiant 1° la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises ; 2° la loi modifiée du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs (ci-après le « projet de loi »)[284].

3. En date du 15 décembre 2023, la Commission nationale a rendu son avis complémentaire sur une série d'amendements parlementaires au projet de loi, approuvée par la Commission de la Justice dans sa séance du 21 juin 2023[285].

4. Lors de sa réunion du 18 avril 2024, la Commission de la Justice a adopté une nouvelle série d'amendements parlementaires (ci-après les « amendements »). Par courrier du 29 avril 2024, Madame la Ministre de la Justice a invité la CNPD à se prononcer sur les amendements audit projet de loi.

I. Ad amendements n°2 et n°8

5. Il y a lieu de saluer les auteurs des amendements pour avoir énuméré les

[284] Délibération n°26/AV13/2023 du 31 mars 2023 de la Commission nationale pour la protection des données, document parlementaire n°7961/04.
[285] Délibération n°104/AV44/2023 du 15 décembre 2023 de la Commission nationale pour la protection des données, document parlementaire n°7961/07

ANNEXES

fichiers des administrations et services publics auxquels le gestionnaire du registre de commerce et des sociétés et du registre des bénéficiaires effectifs (ci-après le « gestionnaire » ou le « LBR ») pourrait avoir accès dans les limites des missions qui lui sont dévolues, dans le cadre de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises (ci-après la « loi RCS »)[286] et la loi modifiée du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs (ci-après la « loi RBE »)[287].

Ces amendements précisent que cet accès pourrait être fait à des fins de vérifications des informations inscrites au registre de commerce et des sociétés (ci-après le « RCS ») ou au registre des bénéficiaires effectifs (ci-après le « RBE »), et de tenue à jour des informations y inscrites. Il convient de féliciter les auteurs des amendements pour de telles précisions.

II. <u>Ad amendement n°6</u>

6. L'amendement n°6 vise à compléter l'article 11 de la loi RBE (article 36 du projet de loi) suite à l'opposition formelle formulée par le Conseil d'État dans son avis complémentaire du 6 février 2024[288].

Les auteurs des amendements ont ainsi complété les dispositions de l'article 11 précité en précisant que l'accès au RBE est également possible pour les journalistes et associations établis dans l'Union européenne qui ont *« un intérêt légitime dans le cadre de la lutte contre le blanchiment et contre le financement du terrorisme ».*

7. Concernant l'absence de définition de la notion d'intérêt légitime dans le texte sous avis, la CNPD renvoie à ses observations formulées au point 36 de son avis complémentaire du 15 décembre 2023[289].

8. Par ailleurs, la Commission nationale se permet de réitérer ses observations formulées dans son avis complémentaire précité selon lesquelles elle *« rappelle que toute diffusion des données à caractère personnel obtenues grâce à l'accès des journalistes professionnels au RBE devra contribuer à un débat d'intérêt général (ici, dans le cadre de la lutte contre le blanchiment et contre le financement du terrorisme) et non pas uniquement à satisfaire la curiosité d'un certain lectorat en dehors des finalités pour lesquelles le RBE a été mis en place »*[290].

9. Les auteurs des amendements précisent encore qu'il est profité de l'occasion *« pour ajouter au point 3° du paragraphe 2 une précision quant aux personnes qui envisagent de conclure une transaction avec une entité immatriculée en y insérant la précision prévue dans la toute prochaine*

[286] Amendement n°2
[287] Amendement n°8
[288] Avis 60.918 du Conseil d'État du 6 février 2024, document parlementaire n°7961/08.
[289] Délibération n°104/AV44/2023 du 15 décembre 2023 de la Commission nationale pour la protection des données, document parlementaire n°7961/07.
[290] Délibération n°104/AV44/2023 du 15 décembre 2023 de la Commission nationale pour la protection des données, document parlementaire n°7961/07, point 35, page 9.

6ième directive AML qui énonce à l'égard de celles-ci que la demande de consultation doit être guidée par le fait que ces personnes veulent éviter tout lien entre les transactions qu'elles entendent conclure et le blanchiment et le financement du terrorisme ». Il convient de saluer ces précisions.

III. <u>Remarques finales</u>

10. Dans la mesure où un certain nombre de développements formulés par la CNPD au sujet des dispositions relatives au projet de loi, et plus particulièrement les dispositions relatives au volet RBE, n'ont pas été prises en compte, la Commission nationale se permet de renvoyer à l'ensemble de ses développements figurant dans son avis complémentaire du 15 décembre 2023, sous le point I intitulé « les amendements à la loi modifiée du 13 janvier 2019 instituant un registre des bénéficiaires effectifs »[291].

Ainsi adopté à Belvaux
en date du 16 mai 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[291] Délibération n°104/AV44/2023 du 15 décembre 2023 de la Commission nationale pour la protection des données, document parlementaire n°7961/07, I, pages 3 à 15.

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8193 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

Délibération n°30/AV/14/2024
du 16 mai 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

2. Par courrier reçu le 6 avril 2023, Monsieur le Ministre de la Sécurité intérieure a invité la Commission nationale à se prononcer sur le projet de loi n°8193 portant modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale (ci-après le « projet de loi »).

3. Selon l'exposé des motifs, les principaux objectifs du projet de loi sont, d'une part, la création d' « une base légale pour la transmission d'informations spontanées du Ministère public vers la Police grand-ducale pour ce qui concerne les procès-verbaux ou autre établis à l'égard d'un membre de la Police grand-ducale », et d'autre part, la réforme de l'enquête d'honorabilité des candidats postulant pour le cadre policier de la Police grand-ducale et l'instauration d'un contrôle d'honorabilité pour les candidats se présentant à des postes dans le cadre civil de la Police.

4. Le présent avis se concentrera sur ses observations concernant les aspects liés à la protection des données, plus particulièrement sur les articles 1 à 4 du projet de loi. Il prendra également en considération l'avis du Parquet général du 4 mai 2023, l'avis du Parquet du Tribunal d'arrondissement de Luxembourg du 9 juin 2023, ainsi que l'avis du Conseil d'État du 28 novembre 2023.

5. Tout d'abord, il convient de saluer la volonté et l'effort des auteurs du projet de loi d'encadrer l'enquête d'honorabilité qui serait effectuée dans le cadre de l'embauche d'un candidat à l'une des fonctions du cadre policier et du cadre civil. En effet, les dispositions envisagées sont plus précises que celles en place actuellement.

III. Sur la transmission d'informations spontanée du ministère public vers la Police grand-ducale prévu par l'article 1er du projet de loi

6. En premier lieu, l'article 1 du projet de loi prévoit que *« le ministère public transmet, de sa propre initiative, au directeur général de la Police, une copie des procès-verbaux ou rapports établis par la Police à l'égard d'un membre de la Police, respectivement des jugements prononcés à l'égard d'un membre de la Police, si le procureur d'État compétent estime que la transmission du procès-verbal, du rapport ou du jugement est opportune ».*

7. Il convient de féliciter les auteurs du projet de loi pour avoir établi, du point de vue de la sécurité juridique, une base légale pour la transmission spontanée de procès-verbaux contenant des données personnelles des membres de la Police du ministère public à la Police grand-ducale.

8. Malgré l'encadrement juridique fourni par cette base légale régissant le transfert d'informations spontanées entre les acteurs susmentionnés, ainsi que les documents qui peuvent en faire l'objet, la Commission nationale souligne que certains aspects liés au traitement des données ne sont pas suffisamment détaillés, voire ne sont pas du tout précisés dans le projet de loi. Cela concerne notamment les critères permettant de déterminer dans quels cas le procureur d'État compétent estime la transmission comme étant « opportune ».

9. Aucune précision n'est fournie concernant les critères ou conditions permettant de déterminer si une telle transmission d'informations spontanée est considérée comme « opportune » ou non. Cette lacune soulève des préoccupations en matière de sécurité juridique et de transparence, notamment pour les personnes concernées.

10. Il en résulte que la CNPD rejoint l'avis du Conseil d'État du 28 novembre 2023, mettant en évidence le manque de précision du champ d'application de ladite disposition et soulignant qu'elle accorde une marge de manœuvre trop importante au procureur d'État.[292]

11. Afin de respecter le principe constitutionnel de prévisibilité et de précision auquel tout texte légal ou règlementaire doit répondre, il est d'une importance primordiale que les auteurs du projet de loi spécifient les critères qui doivent être pris en considération pour déterminer si un procès-verbal ou un jugement concernant un membre de la police peut faire l'objet d'une transmission du ministère public vers la Police grand-ducale.[293]

12. La CNPD considère comme essentiel que les auteurs du projet de loi apportent des précisions sur ces points. Elle rappelle également que seules les données nécessaires et pertinentes peuvent être communiquées.

IV. Quant à l'article 2 du projet de loi portant création du nouvel article 54-1 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale

[292] Voir avis du Conseil d'État du 28 novembre 2023, doc.parl. 8193/03 (ci-après « avis du Conseil d'État »), page 2
[293] Voir point A, page 11 de la délibération n°3/AV3/2021 du 10/02/2021.

ANNEXES

13. En deuxième lieu, l'article 2 du projet de loi sous avis prévoit que *« […] lorsqu'un membre de la Police est soupçonné d'être impliqué dans les faits pénaux ou des faits qui font craindre que ce dernier constitue un danger pour soi-même ou pour autrui, le membre de la Police constatant doit en informer sans délai le directeur général de la Police ».*

14. La Commission nationale observe que cet article impose aux agents de la Police grand-ducale la responsabilité de signaler tout soupçon de faits pénaux ou de troubles mentaux concernant leurs collègues au directeur général de la Police. Cette disposition introduit une nouvelle obligation pour tous les membres de la Police grand-ducale, comme précisé par le Conseil d'État dans son avis.[294]

15. Tout comme l'a souligné le Parquet du tribunal d'arrondissement dans son avis[295], la CNPD peut comprendre que cette nouvelle obligation imposée aux membres de la Police grand-ducale vise à répondre à un « besoin réel », permettant ainsi au directeur général de faire face, sans délai, aux situations envisagées par la disposition en question. Cependant, la CNPD tient également à mettre en évidence la problématique de la prévisibilité de cette mesure.

16. En effet, la CNPD déplore le manque de précision dans le texte du projet de loi qui ne prévoit pas ce qui pourrait relever des situations *« qui font craindre que ce dernier constitue un danger pour soi-même ou pour autrui ».* De même, le texte de de loi, ni le commentaire des articles, n'évoquent de manière précise les mesures conservatoires envisageables que le directeur général de la Police pourrait prendre dans de telles circonstances.

17. En ce qui concerne le champ d'application de la disposition, la CNPD observe, à la lecture du commentaire des articles, que les auteurs du projet de loi proposent des exemples concrets qui pourraient être couverts par cette mesure, tels que les cas de violence domestique ou de tendances suicidaires.

18. Dans le cas de transmission d'informations relatives à des tendances suicidaires, le membre de la Police signalant les faits et le directeur général de la Police seraient amenés, le cas échéant, à traiter des données relatives à la santé des agents, qui constituent des catégories particulières de données à caractère personnel au sens de l'article 9 du RGPD, dites « données sensibles »de.[296] Or, cette disposition prévoit une interdiction de principe de traiter de telles données, à moins de pouvoir justifier le recours à l'une des conditions restrictives de l'article 9 paragraphe 2. Il s'ensuit qu'une telle transmission de données sensibles devrait être explicitement mentionnée dans la loi, accompagnée des garanties appropriées pour les personnes concernées.

[294] Voir avis du Conseil d'État du 28 novembre 2023, doc.parl. 8193/03 (ci-après « avis du Conseil d'État »), page 3
[295] Voir avis du Parquet du Tribunal d'arrondissement du 4 mai 2023, doc.parl. 8193/01 (ci-après « avis du Parquet du tribunal d'arrondissement »)
[296] Voir point V, page 29 de la délibération n°3/AV3/2021 du 10/02/2021.

19. Dans la continuité de cette réflexion, la Commission nationale se questionne sur l'opportunité d'incorporer directement dans le texte de loi une liste exhaustive de cas de figure, ou au moins des conditions précises déclenchant la procédure d'urgence décrite. Cette démarche permettrait d'établir un cadre juridique plus prévisible et contribuerait à clarifier les contours d'application de la disposition, offrant ainsi aux agents policiers une orientation plus claire sur les circonstances qui pourraient justifier un signalement en vertu de cette disposition.

20. Or, en l'absence de telles précisions dans le texte du projet de loi, il sera difficile pour les agents policiers d'apprécier quels cas pourraient donner lieu à un signalement au directeur général de la Police. La CNPD se demande si la disposition en question ne pourrait pas conduire à des signalements arbitraires.

V. Observations sur l'enquête d'honorabilité des candidats du cadre policier et du cadre civil au sein de la Police grand-ducale

21. L'article 3 du projet de loi sous examen a pour objectif d'instaurer une procédure de vérification de l'honorabilité des candidats postulant au sein du cadre policier de la Police grand-ducale. L'article 4 du même projet de loi prévoit un contrôle d'honorabilité pour tout candidat au sein du cadre civil.

22. La CNPD tient à saluer l'initiative visant à intégrer la vérification de l'honorabilité au sein du cadre civil, une avancée pour combler une lacune identifiée par les auteurs du projet de loi. Cette démarche permettra de mieux encadrer l'accès des agents du cadre civil à divers fichiers contenant des données à caractère personnel, y compris des données sensibles liées aux activités policières.

23. La Commission nationale souhaite toutefois attirer l'attention des auteurs du projet de loi sur une question qu'elle a déjà abordée dans ses avis antérieurs concernant les enquêtes d'honorabilité[297], relative au changement du cadre législatif initial applicable aux données. En effet, les données initialement régies par la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale seraient désormais soumises au RGPD en raison de leur utilisation à des fins de recrutement.[298]

24. En outre, bien que les articles 3 et 4 du projet de loi sous examen établissent les procédures de vérification des antécédents ou de « contrôle d'honorabilité » des candidats au cadre policier et civil, précisent les types de données traitées, les personnes concernées ainsi que la durée de conservation des données à caractère personnel, la Commission nationale tient cependant à souligner que certains éléments

[297] Voir notamment nos avis sur le PL7691 (délibération n°3/AV3/2021 du 10/02/2021 et délibération n°42/AV20/2022 du 7/10/2022), sur le PL7425 (délibération n°42/2019 du 8/07/2019, délibération n°2/2021 du 4 février 2021 et délibération n°29/AV24/2021 du 1/10/2021), sur le PL7863A (délibération n°43/AV21/2022 du 7/10/2022 et délibération n°56/AV28/2022 du 2/12/2022).

[298] Voir point II, page 7 de la délibération n°3/AV3/2021 du 10/02/2021.

ANNEXES

relatifs au traitement des données ne sont pas suffisamment détaillés, voire ne le sont pas du tout, dans le projet de loi.

25. Ainsi, aux fins de vérifier l'honorabilité du cadre policier, le projet de loi prévoit dans son article 3, paragraphe (1), points 1° et 2° que le contrôle effectué portera sur *« les faits suivants ayant fait l'objet d'une condamnation pénale ou qui ont donné lieu à l'établissement d'un procès-verbal ou d'un rapport de police [...] un ou plusieurs faits incriminés en tant que crime ou délit par la loi »* ainsi que *« les faits visés à l'article 563, point 3°, du Code pénal relatif aux voies de fait et violences légères. L'alinéa 2 ne s'applique pas aux faits qui, bien que relevant des point 1° et 2°, ont fait l'objet d'un acquittement, d'une décision de non-lieu, d'une réhabilitation judiciaire ou légale, ou sont prescrits. »*

26. Or, il est à noter que sur le site internet de la Police[299], la liste des infractions est plus détaillée :

« L'enquête de moralité comprend une consultation du fichier central. Les faits commis en tant que majeur qui peuvent mener à un refus à l'admission au stage sont notamment les suivants :
- *Consommation régulière de stupéfiants ;*
- *Affaires de violence physique (coups et blessures volontaires) ou psychique (menaces, injures) ;*
- *Rébellion ;*
- *Défaut de suivre les injonctions de la Police, se soustraire à un contrôle de Police ».*

27. Si l'omission d'une liste exhaustive des infractions dans la loi est compréhensible, la Commission nationale se demande s'il ne serait pas judicieux de préciser ces infractions, au moins dans le commentaire des articles ou éventuellement à travers un règlement grand-ducal ?

28. Par ailleurs, en vue d'effectuer le contrôle susmentionné, l'article 3, alinéa 4, pour le cadre policier ainsi que l'article 4, paragraphe (2), alinéa 2 pour le cadre civil, disposent que « la Police consulte les données à caractère personnel du candidat contenues dans le fichier central ainsi que les fichiers qui lui sont légalement accessibles pour autant que cette consultation est pertinente quant à la finalité recherchée. »

29. Or, la Commission nationale se demande quels sont les fichiers visés par cette disposition. S'agirait-il des fichiers listés dans l'article 43 de la loi modifiée du 18 juillet 2018 relative à la Police grand-ducale ? Si tel était le cas, se poserait alors la question de la réelle nécessité de consulter l'ensemble de ces fichiers. À titre d'exemple, on peut se se demander si la consultation du fichier des étrangers ou des demandeurs d'asile est véritablement nécessaire.

30. Si, dans la pratique, seul le fichier central est effectivement consulté, il conviendrait de supprimer cette référence à d'autres fichiers « légalement accessibles ». Si d'autres fichiers sont effectivement consultés dans le cadre de l'enquête d'honorabilité, il serait judicieux de dresser une liste limitative de ces fichiers.

[299] Voir le site internet de la Police grand-ducale, « Devenir policier dans le groupe de traitement A1 » https://police.public.lu/fr/recrutement/cadre-policier/a1.html

31. En l'absence de telles précisions, il est difficile d'apprécier si le principe de minimisation des données est respecté. Il est à rappeler que, conformément à ce principe, seules les données à caractère personnel strictement nécessaires à la réalisation des finalités poursuivies peuvent être utilisées et consultées par la Police.

32. La CNPD se questionne plus particulièrement sur la consultation éventuelle du registre spécial des mineurs. Si une telle consultation est envisagée, elle devrait être dûment justifiée et explicitement précisée dans le texte législatif. De plus, elle devrait être conforme aux dispositions du projet de loi n°7991 actuellement en cours, notamment à l'article 57 tel qu'amendé. À ce stade, il semble que cette consultation soit envisagée uniquement pour les services spécialisés du Service de Police judiciaire, notamment la section de la délinquance juvénile, de la protection de la jeunesse et des infractions à caractère sexuel.

33. Par ailleurs, l'article 3, paragraphe (3) du projet sous examen vise un éventuel échange de renseignements entre le directeur du Service de renseignement de l'État (ci-après le « SRE ») et le directeur général de la Police grand-ducale dans le cadre du recrutement policer.

34. Cette disposition pose la question de la transmission de documents classifiés par le SRE à la Police. En l'absence de clarification sur les modalités de cet échange, la CNPD n'est pas en mesure d'évaluer la conformité de ces échanges avec le RGPD ou 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. Dans ce contexte, la CNPD renvoie à ses interrogations concernant les interactions entre ladite loi et le RGPD, alors que les données traitées par le SRE relèvent initialement du champ d'application matériel de ladite loi.

35. Concernant le transfert de données entre le SRE et le directeur général de la Police grand-ducale, ainsi que l'articulation entre l'application du RGPD et d'autres législations nationales, la CNPD renvoie aux observations détaillées formulées dans son avis du 10 février 2021 (délibération n°3/AV3/2021).[300] Ces observations fournissent des éclaircissements sur ces questions et devraient être prises en considération dans l'élaboration et la mise en œuvre du projet de loi sous examen.

36. Finalement, quant aux durées de conservation des données dans le cadre du recrutement policier et civil, le projet sous avis, prévoit dans l'article 3, paragraphe (6) pour le recrutement au cadre policier et dans l'article 3, paragraphe (5) du même texte pour le cadre civil que les données personnelles des candidats « sont détruits six mois à compter du jour où la décision sur la candidature a acquis force de la chose décidée ou jugée ».

37. La CNPD salue la volonté des auteurs du projet de définir une durée de conservation des données personnelles en accord avec

[300] Voir point III, page 14 et point IX, page 33 de la délibération n°3/AV3/2021 du 10/02/2021.

ANNEXES

les exigences du RGPD. Cependant, ces détails ne suffisent pas à permettre à la Commission nationale d'évaluer dans quelle mesure, dans ce cas précis, le principe de conservation limitée des données serait respecté conformément aux exigences du RGPD.

38. La Commission nationale suppose que cette durée de six mois a été définie par analogie à la législation relative à l'armée. Toutefois, il conviendrait de fournir des explications supplémentaires sur la pertinence de cette durée par rapport aux besoins propres de la Police en matière de contrôle d'honorabilité des candidats. Bien que le projet de loi définisse la durée de conservation des données, le commentaire des articles devrait donc préciser les critères utilisés pour établir cette durée de six mois, et ainsi permettre à la CNPD d'évaluer la proportionnalité de cette durée de conservation par rapport aux données personnelles collectées lors des enquêtes d'honorabilité.

Ainsi adopté à Belvaux
en date du 16 mai 2024.

La Commission nationale
pour la protection des données

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

6

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n° 7994 portant aide, soutien et protection aux mineurs, aux jeunes adultes et aux familles portant modification : 1. du Code du travail ; 2. du Code de la sécurité sociale ; 3. de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ; 4. de la loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'État ; 5. de la loi modifiée du 4 juillet 2008 sur la jeunesse ; 6. de la loi modifiée du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 7. de la loi du 1er août 2019 concernant l'institut étatique d'aide à l'enfance et à la jeunesse ; et portant abrogation 1. de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse ; 2. de la loi modifiée du 16 décembre 2008 relative à l'aide à l'enfance et à la famille

Délibération n°31/AV15/2024
du 16 mai 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

2. Le 13 janvier 2023, la Commission nationale a rendu un avis[301] relatif au projet de loi n°7994 portant aide, soutien et protection aux mineurs, aux jeunes et aux familles et portant modification : 1. du Code du travail ; 2. de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ; 3. de la loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'État ; 4. de la loi modifiée du 4 juillet 2008 sur la jeunesse ; 5. de la loi modifiée du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux; 6. de la loi du 1er août 2019 concernant l'institut étatique d'aide à l'enfance et à la jeunesse ;

[301] Délibération n°5/AV1/2023 du 13 janvier 2023 de la Commission nationale pour la protection des données, doc. parl. n° 7994/09 (ci-après l' « avis initial »).

ANNEXES

et portant abrogation 1. de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse ; 2. de la loi modifiée du 16 décembre 2008 relative à l'aide à l'enfance et à la famille (ci-après le « projet de loi »).

3. Par courrier en date du 20 février 2023, Monsieur le Ministre de l'Éducation nationale, de l'Enfance et de la Jeunesse a invité la Commission nationale à se prononcer sur les amendements gouvernementaux au projet de loi qui ont été approuvés par le Conseil de gouvernement dans sa séance du 8 février 2023 (ci-après les « amendements gouvernementaux »).

4. En outre, le ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse a transmis à la CNPD le 23 février 2023 quatre projets de règlements grand-ducaux[302] qui sont censés compléter le projet de loi.

5. La Commission nationale note que les amendements gouvernementaux prennent en compte certaines des observations formulées dans son avis initial. Il est toutefois à regretter que le titre VII du projet de loi, dédié à la protection des données, reste inchangé.

6. Le présent avis complémentaire se prononcera sur les amendements gouvernementaux ainsi que sur les dispositions des projets de règlements grand-ducaux touchant à la protection des données à caractère personnel. Au vu des nombreuses oppositions formelles formulées par le Conseil d'État dans son avis du 1er juin 2023[303] qui, si le législateur souhaite en tenir compte, nécessitent un remaniement du texte, la CNPD se dispensera d'un examen détaillé et se limitera à formuler des observations d'ordre général.

XXIII. Sur la maison de l'accueil en famille et la procédure de sélection des familles d'accueil

7. Dans son avis initial, la Commission nationale regrettait que le projet de règlement grand-ducal fixant notamment la procédure afférente à la sélection des familles d'accueil n'ait pas été joint au projet de loi. Par la suite, elle s'est vu transmettre le projet de règlement grand-ducal concernant les familles d'accueil qui, selon son exposé des motifs, vise à préciser quatre volets de l'accueil en famille d'accueil, à savoir la procédure de sélection des accueillants, la formation des accueillants, les conditions d'agrément et le dispositif de l'assurance de la qualité des services.

8. Sans vouloir procéder à un examen détaillé de ce texte, la CNPD constate que le projet de règlement grand-ducal concernant les familles d'accueil prévoit un certain nombre de dispositions, telles que l'article 8

[302] Il s'agit des textes suivants : 1. Projet de règlement grand-ducal précisant le financement des mesures d'aide, de soutien et de protection aux mineurs, aux jeunes adultes et aux familles ; 2. Projet de règlement grand-ducal concernant les familles d'accueil ; 3. Projet de règlement grand-ducal fixant la composition, l'organisation et le mode de fonctionnement du conseil supérieur de l'aide, du soutien et de la protection aux mineurs, aux jeunes adultes et aux familles ; 4. Projet de règlement grand-ducal concernant les mesures d'aide de soutien et de protection aux mineurs, aux jeunes adultes et aux familles, l'agrément à accorder aux prestataires des mesures et le dispositif de l'assurance de la qualité des services.

[303] Avis 60.980 du 1er juin 2023 du Conseil d'État, doc. parl. n°7994/21.

relatif au dossier de candidature ou encore l'article 9 relatif au contrôle d'honorabilité, qui constituent des limitations au droit à l'autodétermination informationnelle et à la protection des données à caractère personnel. Ces dispositions relèvent d'une matière réservée à la loi en vertu des articles 31 et 37 de la Constitution. D'après la jurisprudence de la Cour constitutionnelle, l'article 45.2 de la Constitution exige que dans ces matières, *« la fixation des objectifs des mesures d'exécution doit être clairement énoncée, de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi »*[304]. Au regard du silence du projet de loi quant à la procédure de sélection des familles d'accueil, le projet de loi risque ne pas être conforme aux exigences de la Constitution.

9. En ce qui concerne l'article 8 du projet de règlement grand-ducal concernant les familles d'accueil, il y a lieu de constater que figure parmi les documents que le dossier de candidature doit comprendre un extrait du registre spécial pour mineurs des personnes mineures ayant 14 ans accomplis faisant partie du ménage. La CNPD se demande si cette disposition est compatible avec le projet de loi n°7991[305] qui énumère de manière limitative les autorités pouvant accéder audit registre ainsi que les finalités pour lesquelles il peut être accédé.

10. L'article 9 du projet de règlement grand-ducal concernant les familles d'accueil a trait au contrôle d'honorabilité. En particulier, il ressort de l'alinéa 1er que l'honorabilité *« s'apprécie sur base des antécédents judiciaires, des informations obtenues auprès du ministère public et de tous les éléments fournis par l'instruction administrative ».* L'alinéa 2 prévoit par ailleurs la production d'un extrait des bulletins numéros 3 et 5 du casier judiciaire, voire du registre spécial pour mineurs pour lequel se pose de nouveau la question de la conformité avec le projet de loi n°7991. La CNPD comprend que le ministre ne se baserait pas uniquement sur les inscriptions au casier judicaire mais qu'il pourrait également obtenir des « informations » auprès du ministère public. Cependant, ces « informations » ne sont pas détaillées par le projet de règlement grand-ducal. S'agit-il d'informations contenues dans les rapports de police ou procès-verbaux ? S'agit-il d'informations relatives à des faits faisant l'objet d'enquêtes ou d'instructions en cours ? A quels types d'infractions pénales les informations se rapporteraient-elles ?

Une attention particulière devrait être portée au fait qu'il s'agisse de données collectées initialement par le ministère public à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions

[304] Cour constitutionnelle, 4 juin 2021, n° 166 et Cour constitutionnelle, 3 mars 2023, n° 177.
[305] Projet de loi portant introduction d'une procédure pénale pour mineurs et portant modification : 1° de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire ; 2° de la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre États membres de l'Union européenne ; 3° de la loi du 20 juillet 2018 portant réforme de l'administration pénitentiaire.

ANNEXES

pénales qui sont soumises, à ce titre, 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. Ces données seraient traitées, dans le cadre du présent projet de loi, à des fins administratives pour des finalités ultérieures différentes et donc soumises au RGPD. La CNPD renvoie à ses observations formulées dans son avis relatif au projet de loi n°7691 ayant 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[306].

11. L'article 21 du projet de règlement grand-ducal concernant les familles d'accueil prévoit que la famille d'accueil procède au recueil de l'opinion des bénéficiaires accueillis. Même si cette disposition reste (trop) vague quant aux informations recueillies, il peut en être déduit que les familles d'accueil seront amenées à traiter des informations personnelles des bénéficiaires et devront veiller, en tant que responsables du traitement, au respect des principes énoncés par le RGPD. Ne serait-il pas préférable de confier cette tâche directement à l'Office national de l'enfance (ci-après l' « ONE »), d'autant plus que les auteurs expliquent dans le commentaire de l'article que les bénéficiaires *« peuvent communiquer leur opinion par rapport à la prise en charge, leurs inquiétudes et leurs souhaits à l'ONE. Ces informations permettent à l'ONE d'approcher les accueillants proactivement avec des conseils, d'identifier des problèmes potentiels rapidement et d'améliorer l'offre de formations continues offertes par la maison d'accueil. »* ?

XXIV. Sur la cellule de recueil des informations préoccupantes

12. La Commission nationale regrette que les amendements gouvernementaux n'apportent pas de précisions ni sur les informations que la cellule de recueil des informations préoccupantes (ci-après la « CRIP ») sera amenée à transmettre, ni sur les organismes auxquels ces informations seront transmises. Elle se joint à l'avis du Conseil d'État[307] ainsi qu'à l'avis commun complémentaire des autorités judiciaires[308] et estime qu'il est primordial de préciser les points 5° et 6° de l'article 36.1 du projet de loi amendé.

13. Par ailleurs, contrairement au texte du projet de loi initial, les amendements gouvernementaux prévoient une obligation (et non plus seulement une faculté) pour toute personne de communiquer à la CRIP une information préoccupante relative à un mineur, et cela nonobstant toute règle de confidentialité, de secret professionnel ou de secret de l'instruction

[306] Délibération n°3/AV3/2021 du 10 février 2021 de la Commission nationale pour la protection des données, doc. parl. n°7691/03, point III.
[307] Avis 60.980 du 1er juin 2023 du Conseil d'État, doc. parl. n°7994/21, p. 12
[308] Avis commun complémentaire de la Cour d'appel, du Parquet Général, des Parquets de Diekirch et de Luxembourg et des Tribunaux d'arrondissement de Diekirch et de Luxembourg du 10 mars 2023, doc. parl. n° 7994/16, p. 4.

lui étant applicable le cas échéant. Les préoccupations formulées par la CNPD aux points 12 à 18 de son avis initial se posent dès lors de manière encore plus aiguë. Les auteurs devraient également veiller à une articulation cohérente avec d'autres dispositions prévoyant une obligation de dénonciation.

XXV. <u>Sur la transparence des décisions</u>

14. L'amendement 19 concernant l'article 49 (article 53 ancien) du projet de loi supprime, sur base de l'avis initial de la CNPD, la référence au délai de 10 jours et à la nécessité de motiver sa demande pour consulter son dossier. En effet, la Commission nationale avait soulevé dans cet avis que le paragraphe 4 de l'ancien article 53 était sans préjudice du droit d'accès qui est prévu à l'article 15 du RGPD et qui n'est soumis à aucune condition de délai ou de motivation.

15. Il est toutefois à noter que le paragraphe 4 de l'article 49 prévoit désormais que « *[d]ans l'intérêt supérieur du mineur, l'ONE peut classer certains passages du dossier comme confidentiels. Cette décision est motivée et est susceptible d'un recours devant le juge de la jeunesse suivant les conditions prévues à l'article 50 de la présente loi. L'avocat du mineur a accès au dossier non-classé.* »
La Commission nationale regrette que le commentaire de l'amendement 19 ne fournisse pas davantage d'explications à cet égard.

16. Elle tient à souligner que l'article 23.1.i) du RGPD permet, par la voie de mesures législatives, de limiter la portée du droit d'accès lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir la protection de la personne concernée ou des droits et libertés d'autrui. L'article 23.2 du RGPD énonce les exigences que toute mesure législative prise sur le fondement de l'article 23.1 doit respecter. Si la volonté des auteurs du projet de loi est de limiter le droit d'accès tel que consacré par l'article 15 du RGPD, et sans préjudice de l'applicabilité de l'exception au droit d'accès prévue à l'article 15.4 du RGPD, il y a lieu de s'assurer que les exigences de l'article 23 du RGPD soient respectées[309].

XXVI. <u>Sur les mesures visant à assurer la qualité des services</u>

17. La Commission nationale regrettait dans son avis initial que le projet de règlement grand-ducal, qui est censé détailler les conditions d'agrément énoncées à l'article 87 (article 91 ancien) de la loi en projet, ne lui ait pas été soumis ensemble avec le projet de loi. Elle s'est vu transmettre par la suite le projet de règlement grand-ducal concernant les mesures d'aide de soutien et de protection aux mineurs, aux jeunes adultes et aux familles, l'agrément à accorder aux prestataires des mesures et le dispositif de l'assurance de la qualité des services.

[309] V. aussi: Comité européen de la protection des données (European Data Protection Board – EDPB), Lignes directrices 10/2020 concernant les limitations au titre de l'article 23 du RGPD, disponibles sous : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en

ANNEXES

18. Ce projet de règlement grand-ducal contient notamment une énumération des documents devant accompagner la demande d'agrément ainsi que des dispositions relatives au contrôle d'honorabilité. Néanmoins, il n'est toujours pas clair comment l'article 87 du projet de loi s'articule avec la loi modifiée du 8 septembre 1998 réglant les relations entre l'État et les organismes œuvrant dans le domaine social, familial et thérapeutique.

19. Par ailleurs, la CNPD note que les dispositions ayant pour objet le contrôle d'honorabilité sont relatives à une matière réservée à la loi en vertu des articles 31 et 37 de la Constitution et renvoie à ses développements sous les points 8 et 10 du présent avis. En ce qui concerne le contrôle d'honorabilité des membres du personnel, la Commission nationale se rallie aux interrogations formulées par le Conseil d'État sur la proportionnalité de la disposition soumettant toute personne travaillant pour le prestataire à des conditions d'honorabilité[310]. S'y ajoute que l'article 24 du projet de règlement grand-ducal est ambiguë, notamment quant à l'entité en charge du contrôle d'honorabilité des membres du personnel. En effet, les alinéas 2 et 3 laissent penser qu'il appartient à l'employeur de contrôler d'honorabilité de son personnel tandis que les alinéas 1er et 4 peuvent être interprétés en ce sens que cette tâche incombe au ministre. Il y a lieu de clarifier ce point.

XXVII. Sur le projet de règlement grand-ducal précisant le financement des mesures d'aide, de soutien et de protection aux mineurs, aux jeunes adultes et aux familles

20. Le projet de règlement grand-ducal précisant le financement des mesures d'aide, de soutien et de protection aux mineurs, aux jeunes adultes et aux familles comporte des dispositions évoquant des traitements de données personnelles. Ainsi, l'annexe 2 intitulée « Lignes directrices en matière d'attribution des accords de prise en charge » indique par exemple que les accords de prise en charge *« sont accordés sur demande motivée au bénéficiaire et au prestataire. Toute demande, y inclus toute demande primaire, demande de changement d'intensité, demande de renouvellement ou demande de la fin de la prise en charge, est appuyée d'une documentation sous forme de rapports sur le bénéficiaire, ses ressources et besoins justifiant la prise en charge et son intensité. Pour certaines prestations une ordonnance médicale est requise. »*

21. La CNPD estime qu'un tel libellé n'est pas suffisamment clair et précis pour permettre aux bénéficiaires de savoir quelles informations les concernant seront traitées. Se pose également la question de savoir si le projet de règlement grand-ducal est conforme à l'article 45.2 de la Constitution en vertu duquel *« [d]ans les matières réservées à la loi par la Constitution, le Grand-Duc ne peut prendre des règlements et arrêtés qu'en*

[310] Avis 60.980 du 1er juin 2023 du Conseil d'État, doc. parl. n°7994/21, p. 24.

6

vertu d'une disposition légale particulière qui fixe l'objectif des mesures d'exécution et le cas échéant les conditions auxquelles elles sont soumises ». À cet égard, il est renvoyé au point 8 du présent avis.

Ainsi adopté à Belvaux
en date du 16 mai 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

ANNEXES

Avis de la Commission nationale pour la protection des données relatif 1. au projet de loi n°8232 relatif à l'autopartage sur la voie publique et portant modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques ; 2. au projet de règlement grand-ducal portant réglementation de l'autopartage sur la voie publique et portant modification : 1° de l'arrêté grand-ducal modifié du 23 novembre 1955 portant règlement de la circulation sur toutes les voies publiques ; 2° du règlement grand-ducal modifié du 26 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 ; 3° du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers

Délibération n°39/AV16/2024
du 21 juin 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement 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 (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Par courriers en date des 11 et 12 mai 2023, Monsieur le Ministre de la Mobilité et des Travaux publics a invité la Commission nationale à se prononcer sur le projet de loi relatif à l'autopartage sur la voie publique et portant modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques (ci-après le « projet de loi »), ainsi que sur le projet de règlement grand-ducal portant réglementation de l'autopartage sur la voie publique et portant modification: 1° de l'arrêté grand-ducal modifié du 23 novembre 1955 portant règlement de la circulation sur toutes les voies publiques ; 2° du règlement grand-ducal modifié du 26 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 ; 3° du règlement grand-ducal modifié du 26 janvier 2016 relatif à la réception et l'immatriculation des véhicules routiers

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

3. Il ressort de l'exposé des motifs que le projet de loi sous examen a notamment pour objectif de « *de créer une base légale pour qu'une commune puisse réserver des places de stationnement sur la voie publique à des véhicules partagés qui sont identifiés comme appartenant à un opérateur d'autopartage agréé par les autorités compétentes et autorisé par la commune en fonction de certains critères de qualité* ». De plus, le projet de règlement grand-ducal a pour objet de fixer et de clarifier les modalités d'obtention d'un agrément d'opérateur d'autopartage, notamment en apportant des précisions sur les pièces à fournir, les procédures et délais. Le projet de règlement grand-ducal prévoit également le contenu essentiel des contrats d'abonnement et des structures tarifaires que l'opérateur d'autopartage propose à ses clients, afin de garantir une transparence maximale et une qualité de service sans discrimination.

4. Bien que la CNPD ait été saisie de manière séparée du projet de loi et du projet de règlement grand-ducal susmentionnés, elle estime qu'il est opportun de traiter les deux projets de texte dans un même avis, étant donné que ces derniers soulèvent des questions similaires ayant trait à la protection des données.

I. Remarques liminaires

5. Il convient de relever que les informations traitées dans le cadre des dispositions des textes sous examen ne sont pas toutes à considérer comme des données à caractère personnel au sens du RGPD. L'article 4.1) du RGPD définit comme données à caractère personnel « *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* ». La Commission nationale tient à souligner que la définition des données à caractère personnel se réfère à des personnes physiques, ainsi le traitement d'informations concernant les personnes morales ne relève en principe pas du champ d'application du RGPD.

6. Le considérant 14 du RGPD dispose que « *[l]e présent règlement 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* ». Cependant, il faut souligner que 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. Dès lors, le RGPD n'aura vocation à s'appliquer que si la loi ou le règlement grand-ducal en projet implique un traitement de données à caractère personnel.

ANNEXES

7. À cet égard, le groupe de travail « article 29 »[311] indique dans son avis 4/2007 sur le concept de données à caractère personnel du 20 juin 2007, WP 136, que *« les informations ayant trait à des personnes morales peuvent également être considérées comme « concernant » des personnes physiques en tant que telles (…). Cela peut être le cas lorsque le nom de la personne morale est dérivé de celui d'une personne physique. Un autre cas de figure est celui du courrier électronique d'une entreprise qui est normalement utilisé par un employé, ou des informations concernant une petite entreprise (du point de vue juridique, un « objet » plutôt qu'une personne morale) qui peuvent éventuellement décrire le comportement de leur propriétaire ».*

II. La mise à disposition des données d'exploitation (Art. 8 du projet de loi)

8. L'article 8 du projet de loi sous examen impose à chaque opérateur d'autopartage de rendre gratuitement disponibles au public certaines données essentielles et de les mettre à jour fréquemment. De plus, le ministre ayant la Circulation routière dans ses attributions (ci-après « le ministre ») peut demander des informations supplémentaires pour évaluer l'efficacité de l'offre d'autopartage et adapter les politiques de mobilité en conséquence.

9. Conformément au premier paragraphe, chaque opérateur d'autopartage doit mettre à la disposition du grand public certaines données, à savoir la localisation géographique des stations d'autopartage, les coordonnées de contact de l'exploitant, la catégorie des véhicules aux stations, le nom de marque et du modèle de véhicules aux stations, la disponibilité des véhicules ainsi qu'un lien vers le canal de distribution de l'opérateur. La Commission nationale tient à souligner qu'il ne s'agit pas de données à caractère personnel et estime que le RGPD n'est pas applicable.

10. Ensuite, selon le deuxième paragraphe, l'opérateur d'autopartage supporte le ministre dans toutes les démarches qui nécessitent une communication directe avec ses clients en vue de mener des enquêtes ciblées dans le but d'améliorer l'efficacité des politiques publiques de mobilité et de quantifier l'impact de l'allocation d'espace publique à l'autopartage. Ces actions incluent la distribution aux clients des informations nécessaires pour participer à l'enquête, l'incitation des clients à y participer, ainsi que l'évaluation de la représentativité de l'échantillon. La Commission nationale regrette que les auteurs du projet de loi ne fournissent pas d'explications sur la manière dont la représentativité de l'échantillon sera évaluée. En outre, elle tient à souligner que l'article 8.2 du projet de loi ne saurait servir de base légale pour des éventuelles transmissions de données personnelles des clients de l'opérateur d'autopartage au ministre. La CNPD comprend que la participation aux enquêtes est volontaire, de sorte que les traitements des données personnelles des clients effectués dans le cadre de ces enquêtes trouveront leur

[311] Le groupe de travail « article 29 » était un organe consultatif qui conseillait la Commission sur les questions de protection des données et qui a contribué à l'élaboration de politiques harmonisées en matière de protection des données dans l'UE. Après l'entrée en application du RGPD le 25 mai 2018, le comité européen de la protection des données a succédé à ce groupe de travail.

base de licéité dans le consentement des personnes concernées, conformément à l'article 6.1.a) du RGPD. Ainsi, le rôle des opérateurs d'autopartage consistera essentiellement à relayer aux clients des informations sur la possibilité de participer à des enquêtes menées par le ministre, tout en respectant les règles applicables en matière de protection des données.

11. Finalement, le ministre peut, conformément au troisième paragraphe, demander aux opérateurs *« des données anonymes sur le nombre, la distance parcourue et la temporalité des déplacements commençant à une ou plusieurs stations, ainsi que des données pseudonymisées sur la fréquence et la temporalité de l'utilisation »*. Ainsi, cette disposition évoque, d'une part, des données anonymes et d'autre part, des données pseudonymisées. D'abord, la CNPD tient à rappeler qu'à l'issue du processus d'anonymisation, le RGPD ainsi que les autres règles en matière de protection des données à caractère personnel ne sont plus applicables. Suivant le considérant 26 du RGPD *« [...] [i]l 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.»*

12. En revanche, la procédure de pseudonymisation doit être considérée comme l'une des mesures techniques et organisationnelles que le responsable du traitement peut être amenée à mettre en place, afin d'atténuer les risques pour les personnes concernées. Conformément à l'article 4.5) du RGPD, la pseudonymisation est définie comme le *« 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. »* En effet, les données à caractère personnel qui ont fait l'objet d'une pseudonymisation peuvent par définition toujours être attribuées indirectement à une personne physique déterminée par le recours à des informations supplémentaires et restent, par conséquent, soumises au RGPD.

13. Selon l'article 8.3 du projet de loi, le ministre peut demander aux opérateurs d'autopartage les données pseudonymisées *« afin d'évaluer l'efficacité de l'offre d'autopartage à des stations particulières sur la voie publique en vue d'adapter l'offre de transports aux besoins de la population et d'assurer l'allocation de l'espace la plus efficace aux modes de transports »*. Comme susmentionné, les données pseudonymisées sont toujours à considérer comme des données à caractère personnel, étant donné qu'il s'agit d'informations concernant une personne physique indirectement identifiable, et le RGPD s'applique intégralement à leur traitement. En vertu du considérant 39 du RGPD *« les données*

ANNEXES

à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. » La Commission nationale s'interroge sur la nécessité de transmettre des données pseudonymisées pour évaluer l'efficacité de l'offre d'autopartage et se demande si l'utilisation des données sous une forme agrégée de façon que les déplacements individuels ne puissent être identifiés ne serait pas suffisante pour atteindre ladite finalité.[312]

14. Dans l'hypothèse où les auteurs du projet de loi souhaiteraient maintenir le principe d'une transmission de données pseudonymisées, se pose la question de la proportionnalité de cette limitation du droit à l'autodétermination informationnelle et à la protection des données à caractère personnel : Est-ce que la finalité poursuivie, à savoir l'évaluation de l'efficacité de l'offre d'autopartage, justifie une limitation de ces droits constitutionnellement protégés? En outre, la Commission nationale estime que le pouvoir du ministre consistant à demander la transmission de données personnelles est insuffisamment circonscrit dans une matière réservée à la loi en vertu des articles 31 et 37 de la Constitution. Ainsi, les données que les opérateurs d'autopartage seraient obligées de transmettre au ministre doivent être précisément et limitativement énoncées au niveau de la loi.

15. Dans ce contexte, il est à noter que l'exposé des motifs du projet de règlement grand-ducal indique que ce texte *« précise également le partage des statistiques des utilisateurs avec les autorités publiques, ce qui peut fournir des informations précieuses pour la planification du trafic et la prise de décision concernant les infrastructures, le stationnement et d'autres sujets qui contribuent à réduire les embouteillages et la pollution atmosphérique. »* Or, le projet de règlement grand-ducal ne contient pas de telle disposition.

III. Les bases de données (Art. 9 du projet de loi)

a) Sur la structure de l'article 9

16. L'article 9 du projet de loi prévoit l'établissement de deux bases de données à caractère personnel. Selon la compréhension de la Commission nationale, l'une est dédiée à la gestion des agréments d'autopartage et l'autre à l'enregistrement des informations spécifiques relatives à la délivrance et la gestion administrative du signe distinctif. Le libellé du projet de loi donne à croire que ce dernier crée ces deux bases de données. Or, la CNPD note que les informations énumérées au paragraphe 4 sont introduites dans une base de données qui existe déjà et pour laquelle le projet de loi prévoit simplement une finalité supplémentaire. En effet, les informations relatives au point 3 du paragraphe 1er sont enregistrées dans la base de données nationale relative aux véhicules immatriculés au Luxembourg, dont la base légale constitue l'article 4.2 de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques.

17. En outre, il est difficile de déterminer quel paragraphe est associé à quelle base de

[312] À toutes fins utiles, la CNPD se permet de renvoyer à l'avis 05/2014 du groupe de travail « Article 29 » sur les techniques d'anonymisation, p. 10, disponible sous : https://cnpd.public.lu/fr/actualites/international/2014/05/G29-anonymisation.html.

données. Il ne ressort pas clairement de la disposition si les mesures visées par les paragraphes 4 à 7 de l'article 9 du projet de loi se rapportent à la base de données relative aux agréments d'autopartage ou bien à la base de données nationale relative aux véhicules immatriculés au Luxembourg. Afin d'assurer une meilleure lisibilité et de renforcer la sécurité juridique, la Commission nationale suggère dès lors de prévoir un article spécifique pour chacune des bases de données respectives. En séparant les dispositions correspondantes, il serait plus aisé de regrouper par exemple les finalités pour chaque base de données ou de mettre en place les mesures de protection de données adaptées.

18. De plus, les auteurs du projet de loi devraient veiller à ce que les dispositions concernant l'enregistrement des informations spécifiques relative à la délivrance et la gestion administrative du signe distinctif prévu à l'article 7 s'articulent de manière cohérente avec les dispositions de la loi précitée du 14 février 1955. La CNPD se demande s'il ne serait pas plus opportun de modifier cette dernière, afin d'y faire figurer la finalité supplémentaire que le point 3° du paragraphe 1er entend introduire.

b) Sur le rôle des différents acteurs

19. La notion de responsable du traitement joue un rôle important dans l'application du RGPD dans la mesure où elle détermine qui est responsable des différentes règles en matière de protection des données ainsi que la manière dont les personnes concernées peuvent exercer leurs droits.[313] Il convient de rappeler que l'article 4.7) 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 ».* En outre, l'article 4.8) 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 ».*

20. Il résulte des paragraphes 6 et 7 de l'article 9 du projet de loi que le *« ministre a la qualité de responsable du traitement conformément aux dispositions de l'article 4, point 7) du [RGPD] »,* et *« la SNCA a la qualité de sous-traitant conformément aux dispositions de l'article 4, point 8), du [RGPD] ».* La Commission nationale se félicite que les auteurs du projet de loi précisent le rôle des différents acteurs dans le cadre de l'article 9 du projet de loi. Cependant, il y a lieu de recommander aux auteurs du projet de loi de préciser dans l'article pour quelle base de données la SNCA agit en tant que sous-traitant du ministre. En effet, la CNPD

[313] V. en ce sens: Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 3., disponibles sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr

ANNEXES

se demande si la SNCA agit en tant que sous-traitant pour les deux bases de données susmentionnées ou bien si les auteurs du projet de loi se réfèrent uniquement à la base de données nationale relative aux véhicules immatriculés au Luxembourg et estime que les explications contenues à cet égard dans le commentaire de l'article 9 n'apportent pas les clarifications nécessaires.

21. Par ailleurs, si ces dispositions visent la base de données nationale relative aux véhicules immatriculés au Luxembourg, se pose la question de savoir s'il ne faudrait pas intégrer ces précisions dans la loi modifiée du 14 mai 1955 concernant la réglementation de la circulation sur toutes les voies publiques. Il est renvoyé au point 18 du présent avis.

c) Sur la durée de conservation

22. La Commission nationale note favorablement que le projet de loi détermine la durée de conservation des données. L'article 9.8 du projet de loi dispose que *« Les données [...] sont conservées pour une durée de cinq ans après la fin de l'agrément ou de l'agrément renouvelé et sont détruites immédiatement dans le cas d'une demande d'agrément refusée. »* Néanmoins, faute d'explications dans le commentaire de l'article quant à la nécessité de conserver les données pendant une durée de cinq ans après la fin de l'agrément ou de l'agrément renouvelé, la CNPD n'est pas en mesure d'apprécier si le principe de limitation de la conservation, conformément à l'article 5.1.e) du RGPD, est en l'espèce respecté.

IV. Quant au projet de règlement grand-ducal

23. L'article 1er du projet de règlement grand-ducal précise la procédure applicable aux demandes d'agrément d'opérateur d'autopartage. Alors même qu'un tel agrément ne peut être accordé qu'à des personnes morales, le projet de règlement grand-ducal prévoit le traitement de données à caractère personnel, telles que les noms et prénoms du représentant légal de la société demanderesse. La CNPD n'a pas d'observations particulières à formuler à cet égard.

24. La CNPD constate toutefois que l'article 3.4.9° du projet de règlement grand-ducal dispose que le contrat d'abonnement *« fixe »* la protection des données à caractère personnel. La Commission nationale tient à rappeler que c'est le RGPD qui fixe les règles applicables en matière de protection des données et qu'un contrat doit contenir des clauses qui respectent les règles et principes du RGPD, comme par exemple, le droit à l'information en fournissant les informations requises en vertu de l'article 13 du RGPD. Ainsi, la Commission nationale invite les auteurs du projet de règlement grand-ducal à reformuler cette disposition.

Ainsi adopté à Belvaux
en date du 21 juin 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Alain Herrmann
Commissaire

6

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

Délibération n°44/AV17/2024
du 28 juin 2024

1. Conformément à l'article 57, paragraphe 1er, lettre (c) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

Par ailleurs, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

2. En date du 27 janvier 2020, la CNPD a avisé[314] le projet de loi n°7511 relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances (ci-après le « projet de loi n°7511 »).

3. En date du 4 juin 2024, des amendements gouvernementaux relatifs audit projet de loi ont été adoptés (ci-après les « amendements »). N'ayant pas été directement saisie par Monsieur le Ministre des Finances, la Commission nationale souhaite néanmoins se prononcer quant aux amendements.

4. Il ressort de l'exposé des motifs que les amendements ont pour objectif d'apporter des ajustements ciblés au projet de loi n°7511, suite à l'avis du Conseil d'État[315], et plus précisément *« à donner suite à l'opposition formelle du Conseil d'État relative au droit d'une entreprise d'assurance ou de réassurance de déroger à une ou plusieurs des mesures spécifiques, destinées à préserver les droits fondamentaux et les intérêts d'une personne concernée par un traitement de données médicales, énumérées sous le point 2 du nouvel article 181-3 (précédemment 181bis) qu'il est proposé d'introduire dans la loi modifiée*

[314] Délibération n°2/2020 du 27/01/2020.
[315] Avis du Conseil d'État du 28 avril 2020, document parlementaire 7511/3.

ANNEXES

du 7 décembre 2015 sur le secteur des assurances. En effet, le Conseil d'État estime qu'un tel dispositif de dérogation dénaturerait in fine l'utilité des mesures de sauvegarde des droits fondamentaux de la personne concernée. »

5. Dès lors, par l'amendement 2, il est proposé de modifier le texte du nouvel article 1er du projet de loi en ce sens que l'entreprise d'assurance ou de réassurance ne puisse plus déroger à l'intégralité des mesures listées sous le point 2 du nouvel article 181-3 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances. Une différence sera ainsi faite entre les mesures auxquelles l'entreprise d'assurance ou de réassurance ne pourra en aucun cas déroger (le chiffrement des données concernant la santé en transit, la mise en place de restriction d'accès et de fichiers de journalisation, ainsi que la sensibilisation du personnel et la mise en place d'une politique interne[316]), d'une part, et celles auxquelles il pourra être dérogé dans le cadre d'une approche basée sur la proportionnalité (désignation d'un délégué à la protection des données, réalisation d'une analyse d'impact relative à la protection des données, l'anonymisation ou la pseudonymisation des données, l'évaluation régulière par un audit indépendant, ainsi que l'adoption de codes de conduite sectoriels[317]), d'autre part.

6. Toute dérogation à cette deuxième catégorie de mesures devra être documentée en interne. En effet, l'obligation de mettre en œuvre toutes les mesures énumérées sous le point 2 du nouvel article 181-3 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances n'aurait jamais pu être respectée ni en théorie, ni en pratique par toute société d'assurances ou de réassurance active sur le territoire luxembourgeois pour tous ses différents traitements de données à caractère personnel et mettrait le secteur de nouveau d'office dans l'illégalité. Le but du projet de loi n°7511, c'est-à-dire mettre un terme à l'insécurité juridique qui pèse sur lesdites sociétés par l'introduction dans le droit national d'une base de légitimité en matière de traitement de données de santé, ne serait alors pas atteint.

7. La CNPD ne peut dès lors que saluer qu'il ne peut pas être dérogé aux mesures prévues aux lettres d), e), f), g) et j) du nouvel article 181-3 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, tandis qu'elle se joint aux explications des auteurs du projet de loi contenues dans le commentaire de l'amendement 2 en ce qui concerne les mesures auxquelles il pourra être dérogé, sous condition de le documenter en interne.

8. Par ailleurs, les amendements introduisent désormais l'obligation de tenir cette documentation sur les éventuelles dérogations à la disposition de la Commission nationale[318], une modification qu'elle ne peut que soutenir.

Il convient de préciser dans ce contexte que conformément à l'article 57.1. a) du RGPD,

[316] Voir les lettres d), e), f), g) et j) du nouvel article 1er, premier alinéa, du projet de loi n°7511.
[317] Voir les lettres a), b), c), h) et i) du nouvel article 1er, premier alinéa du projet de loi n°7511
[318] Voir deuxième alinéa du nouvel article 1er du projet de loi n°7511.

auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la CNPD a comme mission de contrôler l'application du RGPD et de veiller au respect de celui-ci. Elle pourrait dès lors décider de contrôler si les sociétés d'assurances et de réassurance ont respecté leur obligation de documenter et de justifier l'exclusion d'une ou plusieurs des mesures énumérées au point 2 du nouvel article 181-3 de la loi modifiée du 7 décembre 2015 sur le secteur des assurances, en adoptant, le cas échéant, une des mesures correctrices prévues à l'article 58.2 du RGPD.[319]

Ainsi adopté à Belvaux
en date du 28 juin 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[319] L'article 12 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 se réfère quant aux pouvoirs de la CNPD à article 58 du RGPD.

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8089 relatif à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique et au projet de règlement grand-ducal fixant certaines modalités d'application de la loi relative à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique

Délibération n°45/AV18/2024
du 4 juillet 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Des amendements parlementaires relatifs au projet de loi n°8089 relatif à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique ont été adoptés lors de la réunion du 21 mai 2024 de la Commission de l'Enseignement supérieur, de la Recherche et de la Digitalisation (ci-après les « amendements parlementaires »).

3. Par courrier du 4 juin 2024, la Ministre de la Digitalisation a invité la Commission nationale à se prononcer sur les amendements parlementaires.

4. Il convient de préciser que la CNPD n'a pas été saisie initialement afin d'aviser le projet de loi n°8089 relatif à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique (ci-après le « projet de loi »), ni le projet de règlement grand-ducal fixant certaines modalités d'application de la loi relative à la signature électronique des actes en matière administrative et portant modification de la loi du 25 juillet 2015 relative à l'archivage électronique (ci-après le « projet de règlement grand-ducal »).

5. La Commission nationale formulera ci-après ses remarques quant aux amendements parlementaires mais également quant aux dispositions du projet de loi initial qui soulèvent des

problématiques ayant trait à la protection des données à caractère personnel.
Elle entend également commenter les dispositions du projet de règlement grand-ducal qui ont vocation à préciser les mesures techniques et organisationnelles devant être prises dans le cadre de la mise en œuvre de la plateforme sécurisée.

IV. <u>Remarques liminaires</u>

6. Il convient de rappeler que l'article 6.1.e) du RGPD, lu en combinaison avec l'article 6.3 du RGPD, prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect 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.

Dans ce cas de figure, le fondement, c'est-à-dire la mission d'intérêt public en cause, et notamment les finalités des traitements de données doivent ressortir soit du droit de l'Union européenne, soit du droit de l'État membre auquel le responsable du traitement est soumis et ce fondement doit répondre *« à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi ».*

Dans un arrêt récent, la Cour de Justice a par exemple estimé que la *« détermination des finalités et des moyens du traitement et, le cas échéant, la désignation de ce responsable par le droit national peuvent être non seulement explicites, mais également implicites. Dans ce dernier cas de figure, il est néanmoins requis que cette détermination découle de manière suffisamment certaine du rôle, de la mission et des attributions dévolus à la personne ou à l'entité concernée. »*[320].

En droit interne, il est à noter que l'article 31 de la Constitution révisée, applicable depuis le 1er juillet 2023, dispose que *« [t]oute 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. »*

7. Dès lors, en tenant en compte que la protection des données à caractère personnel est une matière réservée à la loi par la Constitution, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc.[321] En effet, d'après la jurisprudence de la Cour constitutionnelle, l'article 45.2 de la Constitution exige que dans ces matières, *« la fixation des objectifs des mesures d'exécution doit être clairement énoncée, de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi »*[322]

[320] CJUE, arrêt du 11 janvier 2024, État belge/Autorité de protection des données, C-231/22, EU:C:2024:7, point 30.
[321] Voir articles 31 et 45 de la Constitution luxembourgeoise.
[322] Cour constitutionnelle, 4 juin 2021, n° 166, Mém. A n°440 du 10 juin 2021 et Cour constitutionnelle, 3 mars 2023, n° 177, Mém. A, n° 127 du 10 mars 2023.

ANNEXES

8. Or, en l'espèce certaines des dispositions sous avis ne respectent pas de telles dispositions. En effet, il est notamment difficile pour certains traitements d'identifier qui est le responsable du traitement ainsi que les finalités des traitements opérés sur la plateforme sécurisée. La CNPD reviendra sur ces points plus en détails *infra*.

V. Sur les actes tombant dans le champ d'application du projet de loi

9. Il convient de constater que les auteurs des amendements parlementaires ont suivi les remarques formulées par le Conseil d'État dans son avis du 12 mars 2024[323] en ce qu'il préconisait la suppression de la définition des « actes en matière administrative »[324].

10. En effet, dans son avis précité, le Conseil d'État a estimé que *« les auteurs [du projet de loi] veulent donner à l'expression « actes en matière administrative » une portée large, visant à la fois les actes émanant de l'administration et ceux que les citoyens adressent à l'administration, « le but du projet étant de couvrir la quasi-totalité des actes susceptibles d'être produits tant entre l'État et ses administrés, qu'entre les différents services étatiques au sens large ». Seuls sont en définitive exclus du champ d'application les actes sous seing privé et les actes authentiques que l'État est amené à passer, et ce au motif que ces actes sont régis par d'autres dispositions légales »* et précise encore qu'il *« se demande si un enchevêtrement de définitions tel qu'il figure au paragraphe 3 de l'article sous examen est véritablement nécessaire pour atteindre l'objectif ainsi décrit. Aux yeux du Conseil d'État, il suffirait pour cela de prévoir dans la loi en projet que « les administrés peuvent signer électroniquement tout acte qu'ils adressent à une autorité administrative ou à une entité exerçant une activité administrative » et que « les autorités administratives et les entités exerçant une activité administrative peuvent signer électroniquement l'ensemble des actes relatifs à l'exercice de leur activité »*[325].

VI. Sur la création d'un identifiant numérique

11. Il y a lieu de relever que la faculté pour les actes, tombant dans le champ d'application du projet de loi sous avis[326], susceptibles de revêtir une signature ou un cachet électronique nécessite la création d'un identifiant numérique.

12. Bien que la CNPD comprenne que l'identifiant numérique se rattacherait à un acte et non à un administré directement, elle tient à rendre attentif les auteurs des amendements parlementaires sur les développements formulés par son homologue français (la Commission nationale de l'informatique et des libertés) dans sa délibération n°2008-578 du 18 décembre 2008 portant avis sur un projet d'arrêté relatif à la création d'un téléservice dénommé « mon.service-public.fr » selon lesquels *« la commission (…) a pris acte que*

[323] V. avis n°61.688 du 22 décembre 2023 du Conseil d'État, document parlementaire n°8089/04.
[324] V. ancien article 1.1 du projet de loi.
[325] V. avis n°61.688 du 22 décembre 2023 du Conseil d'État, document parlementaire n°8089/04.
[326] Voir article article 3 nouveau du projet de loi, tel qu'amendé.

les numéros permettant de relier le portail « mon.service-public.fr » aux sites partenaires choisis par les usagers seraient des chaînes de caractères alphanumériques aléatoires et non signifiantes, permettant seulement de faire le lien entre les téléservices, sans que le système technique MSP ne puisse avoir connaissance des identifiants sectoriels des usagers. Elle constate que « mon.service-public.fr » n'aboutit pas à un regroupement d'identifiants sectoriels autour d'un identifiant commun, et que le projet n'a pas pour objectif ni pour conséquence de créer un identifiant administratif national. Elle estime toutefois que cette question, fondamentale au regard des grands principes de la loi du 6 janvier 1978 modifiée, devrait être garantie par les textes et non pas seulement par des mesures techniques, et que le principe de la fédération volontaire d'identité devrait être explicité. Elle demande ainsi que le projet d'arrêté portant création du portail « mon.service-public.fr » énonce expressément que le dispositif, bien que créant un lien sous le contrôle de l'usager entre différents identifiants sectoriels, ne doit pas conduire à la création d'un « identifiant administratif unique » des usagers ».

VII. Sur les acteurs de la plateforme sécurisée

13. Les dispositions de l'article 3 du projet de loi, tel qu'amendé, précise que *« [t]out acte relatif à l'exercice de leur activité signé ou cacheté électroniquement par les autorités administratives et les entités exerçant une activité administrative, destiné à un administré, doit être pourvu d'un identifiant numérique à des fins de vérification de l'authenticité et conservation de la preuve de la signature ou du cachet électronique »*[327].

14. Ainsi, une plateforme sécurisée a vocation à être créée[328]. Cette plateforme poursuit plusieurs objectifs :

- permettre l'apposition d'un identifiant numérique sur les actes visés par le projet de loi sous avis ;
- permettre la lecture d'un identifiant numérique apposé sur les actes visés par le projet de loi sous avis ;
- vérifier l'authenticité de la signature ou du cachet électronique ; et
- conserver les actes visés par le projet de loi sous avis, signés ou cachetés électroniquement.

15. Cette plateforme serait mise à disposition par le Centre des technologies de l'information de l'État (ci-après le « CTIE ») ou, le cas échéant, par le biais d'une plateforme équivalente, interopérable avec la plateforme sécurisée[329].

16. Le projet de loi, tel qu'amendé, précise que *« [t]oute autorité administrative et entité exerçant une activité administrative ayant demandé la création d'un identifiant numérique conformément à la présente loi a la qualité de responsable du traitement »*[330] et que le CTIE *« ainsi que tout opérateur de toute plateforme équivalente a la qualité de sous-traitant » « dans l'opération de*

[327] V. amendement n°5, nouvel article 3 du projet de loi.
[328] V. amendement n°8, nouvel article 5 du projet de loi.
[329] V. amendement n°7, nouvel article 4 du projet de loi.
[330] V. amendement n°8, nouvel article 5 du projet de loi.

ANNEXES

la plateforme »[331]. La CNPD salue de telles précisions mais souhaiterait attirer l'attention des auteurs des amendements parlementaires sur les points ci-après.

17. En ce qui concerne la détermination du responsable du traitement, le Comité européen de la protection des données précise que *« pour une opération de traitement particulière, le responsable du traitement est l'acteur qui a déterminé la raison pour laquelle le traitement a lieu (c'est-à-dire « à quelles fins » ou « pourquoi ») et comment cet objectif sera atteint (c'est-à-dire quels moyens doivent être mis en œuvre pour atteindre l'objectif) »*[332].

18. La Commission nationale comprend que les autorités ou entités *« exerçant une activité administrative ayant demandé la création d'un identifiant numérique »* auront effectivement la qualité de responsable du traitement alors qu'elles décideront d'avoir recours à cette plateforme pour signer électroniquement les actes, tels que visés par le texte en projet, pour vérifier l'authenticité de la signature ou du cachet électronique et éventuellement conserver lesdits actes signés ou cachetés électroniquement. Le CTIE ne traite ces demandes que sur instructions des autorités et entités précitées, de sorte qu'il agirait par conséquent comme sous-traitant pour ces traitements de données. Cependant, des nuances quant à cette qualification devraient être apportées.

19. En effet, il y a lieu d'attirer l'attention des auteurs des amendements parlementaires sur la notice d'information « Protection des données à caractère personnel » du site internet « guichet.lu » qui précise que pour les *« traitements MyGuichet.lu relatifs à l'identification, (...) et mise à disposition d'un espace de stockage »*, le CTIE est considéré comme responsable du traitement[333].

Dès lors, la CNPD se demande si un parallèle avec la gestion par le CTIE de la plateforme sécurisée sous examen peut être fait avec sa gestion du site « MyGuichet.lu » notamment en ce qui concerne les traitements relatifs à l'identification et la mise à disposition d'un espace de stockage. Le CTIE est-il à considérer comme un responsable du traitement pour certains des traitements prévus par le projet sous examen[334] ?

20. Par ailleurs, en ce qui concerne les traitements opérés aux fins de vérification de l'authenticité de la signature ou du cachet électronique, le CTIE agit-il en tant que simple sous-traitant ou est-ce que ce dernier pourrait être considéré comme conjointement responsable[335] avec l'autorité administrative ou l'entité exerçant une activité administrative, responsable du traitement ?

21. Il est, dès lors, vivement recommandé de procéder à une analyse, pour chaque traitement de données effectué sur la

[331] V. amendement n°8, nouvel article 5 du projet de loi.
[332] Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, adoptées le 7 juillet 2021 par le Comité Européen de la Protection des Données, page 16, point 35.
[333] V. point IV, paragraphes 82 à 87 sur le site internet suivant https://guichet.public.lu/fr/citoyens/support/aspects-legaux.html.
[334] V. article 4 nouveau, amendement 7.
[335] V. article 4.7 du RGPD, et Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, adoptées le 7 juillet 2021 par le Comité Européen de la Protection des Données, point 2.1.3.

plateforme, des rôles joués par les différents acteurs de la plateforme afin de s'assurer de leur qualification juridique exacte, à savoir celle de responsable du traitement, responsables du traitement conjoints ou sous-traitant.

22. En tout état de cause, la Commission nationale estime que les traitements effectués par le CTIE devraient être définis plus précisément par l'article 5.5 du projet de loi. En effet, la formulation suivante *« dans l'opération de la plateforme sécurisée »*, employée par le nouvel article 5.5 du projet de loi, apparaît comme étant trop vague, compte tenu des remarques formulées *supra*.

VIII. Sur les catégories des données et les finalités des traitements de données à caractère personnel

23. Le texte sous avis précise encore que les finalités poursuives par les traitements de données opérés dans le cadre de la plateforme sont les suivantes :

- *« permettre la lecture de l'identifiant numérique, la vérification de l'authenticité de la signature ou du cachet électronique, la conservation des actes signés ou cachetés électroniquement pourvus d'un identifiant numérique et l'accès à l'endroit de stockage par le biais de l'identifiant numérique » ;*
- *« permettre l'apposition de l'identifiant numérique ».*

24. Les catégories de données à caractère personnel amenées à être traitées à ces fins seraient :

- *« le contenu chiffré de tout acte signé ou cacheté électroniquement pourvu d'un identifiant numérique » ;*
- *« l'identité de l'agent de l'autorité administrative ou de l'entité exerçant une activité administrative ayant demandé la création d'un identifiant numérique »*[336].

25. La CNPD comprend que l'ensemble des catégories de données énoncées ci-dessus seraient traitées pour l'ensemble des finalités énumérées ci-avant. Si tel ne devait pas être le cas, il conviendrait, pour une meilleure compréhension, de préciser dans le texte sous examen quelles catégories de données à caractère personnel sont traitées pour quelles finalités.

26. Par ailleurs, la Commission nationale se demande si d'autres catégories de données seraient amenées à être traitées pour les finalités énoncées ci-avant. En effet, est-ce que les catégories de données énumérées au paragraphe 4 du nouvel article 5 du projet de loi ne sont-elles pas traitées pour certaines des finalités énoncées à l'article 5.1 précité ? Bien que celles-ci ne soient pas conservées sur la plateforme, la CNPD comprend que celles-ci pourraient tout de même amenées à être traitées. Des précisions à ce sujet mériteraient d'être apportées par les auteurs des amendements parlementaires.

27. Enfin, il y a lieu d'attirer l'attention des auteurs des amendements parlementaires ainsi que des auteurs du projet de loi sur les règles applicables aux traitements

[336] V. Amendement n°8, nouvel article 5 du projet de loi.

ANNEXES

de catégories particulières de données au sens de l'article 9 du RGPD. Dans l'hypothèse où les actes tombant dans le champ d'application du texte en projet contiendraient de telles données, il convient de rappeler que leur traitement est en principe interdit sauf si l'une des conditions visées au paragraphe 2 dudit article est remplie.

28. Il appartient au responsable du traitement de veiller au respect de telles dispositions et de dès lors s'assurer que, le cas échéant, les traitements de catégories particulières de données respectent l'une des conditions visées au paragraphe 2 dudit article.

IX. Sur les traitements à des fins de « conservation des actes signés ou cachetés électroniquement pourvus d'un identifiant numérique »

29. L'exposé des motifs du projet de loi initial précise que *« [l]'identifiant numérique permet ainsi à tout administré destinataire de l'acte, et à toute administration à laquelle un administré présente une copie de l'acte d'accéder, à l'aide de cet identifiant numérique, au lieu de conservation de l'acte original et d'en prendre connaissance. Il est à noter que les actes sont accessibles sur la plateforme sécurisée ou les plateformes équivalentes, pendant une durée de trente ans »*[337].

30. Il ressort encore du commentaire des articles du projet de règlement grand-ducal que *« [l]a plateforme n'a en effet pas vocation à remplacer les solutions de gestion électronique des documents aujourd'hui utilisées par les autorités administratives et les autres entités, ni d'éventuelles solutions de stockage à long terme de ces actes ».*

31. L'article 3 du projet de loi, tel qu'amendé, précise également que l'apposition de l'identifiant numérique a pour but la *« conservation de la preuve de la signature ou du cachet électronique ».*

32. La CNPD comprend, dès lors, que les actes seraient conservés afin de :
- conserver une preuve de la signature ou du cachet électronique pour les administrés ; et
- permettre aux administrés, autorités administratives ou entités exerçant une activité administrative d'accéder auxdits actes signés ou cachetés électroniquement.

33. En ce qui concerne la conservation de la preuve de la signature ou du cachet électronique, la Commission nationale comprend que la conservation serait nécessaire afin de garantir la valeur probante de tels actes sous forme électronique pour permettre le cas échéant aux administrés de verser de tels actes en tant que preuve lors d'un éventuel litige.

34. Dans la mesure où le CTIE a le statut de Prestataire de Services de Dématérialisation ou de Conservation (ci-après « PSDC ») en vertu des règles prévues par la loi du 25 juillet 2015 relative à l'archivage

[337] V. exposé des motifs du projet de loi initial, page 5.

électronique[338], la Commission nationale se demande si les documents seraient dès lors conservés dans les conditions prévues par la loi précitée ?

35. Enfin, bien que cette solution technique de conservation soit d'après la compréhension de la CNPD mise à disposition des administrés, cela ne serait-il pas également le cas pour les administrations ou entités exerçant une activité administrative (bien qu'il soit précisé par les auteurs du projet de règlement grand-ducal que cette conservation n'a pas vocation *« à remplacer les solutions de gestion électronique des documents aujourd'hui utilisées par les autorités administratives et les autres entités, ni d'éventuelles solutions de stockage à long terme de ces actes »*)[339] ?.

36. Des clarifications quant aux interrogations soulevées par la Commission nationale devraient être apportées.

X. Sur le principe de minimisation des données

37. Les dispositions sous examen précisent qu'en vertu du principe de minimisation des données[340], la plateforme ne conserve pas :

- *« le nom des fichiers contenant les actes signés ou cachetés électroniquement reçus » ;*
- *« le contenu en clair des actes signés ou cachetés électroniquement reçus » ;*
- *« les identifiants numériques générés par la plateforme sécurisée ainsi que toute plateforme équivalente et associés aux actes signés ou cachetés électroniquement » ;*
- *« les données permettant d'identifier les agents ou les administrés ayant accédé à un acte signé ou cacheté électroniquement sur base d'un identifiant numérique »*[341].

38. S'il convient de féliciter les auteurs des amendements parlementaires pour avoir prévu de telles dispositions, il y a lieu de regretter que les raisons ayant poussées les auteurs desdites dispositions à ne pas conserver de telles données, sous couvert du principe de minimisation des données, ne figurent pas dans le commentaire des amendements.

39. De telles justifications seraient les bienvenues. En effet, la CNPD se demande plus particulièrement si les données qui permettraient le traçage des accès aux actes signés ou cachetés électroniquement sont tout de même conservées sur un autre support.

XI. Sur les mesures de sécurité

40. Le responsable du traitement se doit de respecter le principe d'intégrité et confidentialité visé à l'article 5.1.f) du RGPD. Par ailleurs, l'article 32 du RGPD dispose encore que *« le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles*

[338] V. Chapitre 2 de la loi du 25 juillet 2015 relative à l'archivage électronique.
[339] V. point 30 du présent avis.
[340] V. article 5.1.c) du RGPD.
[341] V. Amendement n°8, nouvel article 5 du projet de loi.

ANNEXES

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.

41. Il y a lieu de rappeler qu'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 l'entité concernée, et à quelles données précises cette personne ou ce service aurait accès.

42. 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.

43. Or, les mesures techniques et organisationnelles concernant la mise en œuvre de la plateforme sécurisée ont notamment comme conséquence que *« [l]es identifiants numériques ne sont également pas stockés, et par conséquent l'opérateur de la plateforme n'est pas en mesure seul d'identifier un acte spécifique, ni de déchiffrer les données stockées pour retrouver le contenu des actes reçus. Ceci permet de garantir que la confidentialité des actes publics sera assurée même dans l'éventualité d'une compromission de la sécurité de la plateforme sécurisée. Cela signifie également qu'en cas de perte d'un identifiant numérique, l'acte correspondant stocké sous forme chiffrée sur la plateforme ne pourra définitivement plus être accédé »*[342].

44. En outre, comme évoqué aux développements précédents, ne sont pas conservées sur la plateforme les *« données permettant d'identifier les agents ou les administrés ayant accédé à un acte signé ou cacheté électroniquement sur base d'un identifiant numérique »*[343].

45. Si de telles précisions sont les bienvenues et compréhensibles, la CNPD regrette que les auteurs du projet de règlement grand-ducal n'aient pas précisé comment le responsable ensemble avec le sous-traitant peuvent se conformer aux exigences de l'article 32 du RGPD, notamment en ce qui concerne le traçage des accès. En l'absence de précisions à ce sujet, elle se demande si un traçage des accès est toujours possible ? Quelles seraient les mesures concrètes qui pourraient être prises par le responsable du traitement en cas d'accès illicite aux actes signés ou cachetés électroniquement ?

46. Par ailleurs, la Commission nationale regrette que les modalités techniques d'accessibilité de la plateforme par les administrés et par les autorités administratives ou entités exerçant une activité administrative n'aient pas été détaillées. Des précisions à ce sujet mériteraient d'être apportées.

[342] V. commentaire des articles sous « Ad article 3 » du projet de règlement grand-ducal.
[343] Amendement n°8, nouvel article 5 du projet de loi.

XII. <u>Sur la durée de conservation</u>

47. En vertu du principe de limitation de la conservation, 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[344].

Toutefois, si les données doivent être en principe supprimées dès lors que les finalités du traitement ont été atteintes, cette règle ne suppose pas de supprimer systématiquement les données dès que les objectifs du traitement ont été atteints. En effet, les données à caractère personnel obéissent à un cycle de vie durant lequel les données peuvent avoir plusieurs utilités successives. Cela signifie que pour des mêmes données, des durées différentes peuvent s'appliquer[345].

48. Le projet de loi, tel qu'amendé, entend fixer une durée de conservation de 30 ans en ce qui concerne les données à caractère personnel suivantes :

- le contenu chiffré des actes signés ou cachetés électroniquement et pourvu d'un identifiant numérique ; et
- l'identité de l'agent de l'autorité administrative ou de l'entité exerçant une activité administrative ayant demandé la création d'un identifiant numérique.

49. Or, compte tenu des développements précédents, la Commission nationale se demande si les auteurs des amendements parlementaires ont tenu compte du cycle de vie des données collectées ? En effet, il ressort du texte sous avis que les données collectées sont traitées afin d'apposer une signature ou cachet électronique et permettre aux parties d'y accéder, puis dans un second temps sont conservées afin d'assurer l'authenticité du document signé ou cacheté électroniquement, ce qui permet le cas échéant de permettre aux administrés de verser un tel document en tant que preuve. En outre, la CNPD se demande encore s'il a été tenu compte, afin de déterminer la durée de conservation, des finalités distinctes pour lesquelles les données sont traitées.

Cette analyse devrait être faite afin de respecter au mieux le principe de limitation de conservation. Par ailleurs, des distinctions quant à la fixation de la durée de conservation des données en fonction de leur cycle de vie, ou finalités, devraient également être prises en compte.

50. En ce qui concerne la conservation pour une durée de 30 ans de l'identité de l'agent de l'autorité administrative ou de l'entité exerçant une activité administrative ayant demandé la création d'un identifiant numérique, il y a lieu de se demander si cette durée de 30 ans est adéquate, pertinente et limitée à ce qui est nécessaire au regard des finalités pour lesquelles ces données sont traitées.

51. La Commission nationale se demande si de telles données sont conservées à des fins de traçage des accès ou sont conservées afin de permettre de vérifier l'authenticité de l'acte ?

[344] V. article 5.1.e) du RGPD.
[345] V. « Guide pratique : Les durées de conservation (cnil.fr), version juillet 2020, publié sur le site de la CNIL.

ANNEXES

52. En ce qui concerne la conservation des données sous examen à des fins de preuve, il y a lieu de relever qu'il ressort du commentaire des articles du projet de règlement grand-ducal que la plateforme n'a *« pas vocation à remplacer les solutions de gestion électronique de documents aujourd'hui utilisées par les autorités administratives et les autres entités ou d'éventuelles solutions de stockage à long terme de ces actes »*[346].

53. Les auteurs des amendements parlementaires précisent quant à eux que *« le délai de trente ans correspond au délai de prescription de droit commun. Etant donné que la plateforme sécurisée a comme vocation de conserver la version originale d'un acte administratif signé électroniquement, permettant de vérifier ainsi l'authenticité de l'acte, cette durée de conservation vise à assurer que les administrés peuvent verser les preuves nécessaires pour faire valoir leurs droits dans les mêmes conditions comme s'ils avaient à leur disposition un original sous format papier. En d'autres termes, la disposition vise à assurer une égalité de traitement de tous les administrés sans distinction du format sous lequel un acte leur est transmis ».*

54. La Commission nationale comprend que la durée fixée par le projet de loi sous examen se calque sur la durée de prescription de 30 ans, et cela afin de permettre aux administrés de fournir le cas échéant une preuve de la signature de l'acte signé ou cacheté électroniquement. Cependant il y a lieu de se demander si des durées de prescription plus courtes seraient applicables compte tenu de la grande diversité des actes amenés à être signés ou cachetés électroniquement.

55. Il y a encore lieu d'attirer l'attention des auteurs des amendements parlementaires qu'une solution différente semble avoir été retenue en France. En effet, en France des dispositions légales prévoient pour le téléservice « Service-Public.fr » que *« l'espace de stockage en ligne est placée sous le contrôle et la responsabilité de son titulaire qui peut le clore à tout moment »*[347].

56. Enfin, il résulte de l'ensemble des développements précédents qu'en l'absence de précision quant aux points d'interrogation soulevés par la CNPD, celle-ci n'est pas en mesure d'apprécier si le principe de limitation de la conservation serait respecté en l'espèce.

Ainsi adopté à Belvaux
en date du 4 juillet 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[346] V. commentaire des articles sous « Ad article 3 » du projet de règlement grand-ducal.
[347] V. arrêté du 24 février 2016 portant intégration au site internet « service-public.fr » d'un téléservice permettant à l'usager d'accomplir des démarches administratives en tout ou partie dématérialisées et d'avoir accès à des services d'informations personnalisés.

6

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8330B portant organisation de l'Administration du cadastre et de la topographie et au projet règlement grand-ducal concernant la consultation et la diffusion de la documentation relative à la mensuration officielle, de la documentation cadastrale, de la documentation topographique, du registre national des localités et des rues et des systèmes de référence de coordonnées nationaux gérés par l'Administration d cadastre et de la topographie ; et portant fixation du tarif des redevances 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

Délibération n°51/AV19/2024
du 7 août 2024

1. Conformément à l'article 57.1.c, du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Le projet de loi n°8330 portant organisation de l'Administration du cadastre et de la topographie a vocation à *« consigner la réalité législative actuelle »*, et abroger et remplacer la loi du 25 juillet 2002 précitée. En effet, selon l'exposé des motifs *« [d]epuis la mise en vigueur de la loi du 25 juillet 2002 portant réorganisation de l'administration du cadastre et de la topographie (…) l'administration du cadastre et de la topographie (…) a connu de profondes évolutions qui conduisent vers la modernisation de cette dernière ».*

3. Dans son avis du 27 février 2024, le Conseil d'État a suggéré de scinder le projet de loi précité *« en deux projets de loi distincts, de sorte à prévoir un premier projet de loi qui traite de l'article 18 portant modification de la loi précitée du 19 mars 1988 et un second projet de loi qui porte sur les articles 1er à 17, 19 et 20 relatifs à l'Administration ».*

La Commission des Finances, lors de sa réunion du 6 mars 2024, a décidé de suivre la recommandation du Conseil d'État et de scinder le projet de loi précité en deux projets de loi distincts :

- Le projet de loi 8330A portant modification de la loi modifiée du

ANNEXES

19 mars 1988 sur la publicité foncière en matière de copropriété, qui reprend uniquement l'article 18 du projet de loi 8330 initial ; et
- Le projet de loi 8330B portant organisation de l'Administration du cadastre et de la topographie reprenant les articles restants (ci-après le « projet de loi »).

4. En parallèle, un projet de règlement grand-ducal concernant la consultation et la diffusion de la documentation relative à la mensuration officielle, de la documentation cadastrale, de la documentation topographique, du registre national des localités et des rues et des systèmes de référence de coordonnées nationaux gérés par l'Administration du cadastre et de la topographie ; et portant fixation du tarif des redevances 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 (ci-après le « projet de règlement grand-ducal »), a été élaboré dans le contexte du projet de loi.

5. Enfin, le projet de loi entend entériner le principe de « publicité foncière » afin *« d'expliquer l'objectif de la consultation et de la diffusion des données du registre foncier »*[348]. Par ailleurs, les auteurs du projet de règlement grand-ducal précisent que le but dudit texte est *« d'informer le public de la documentation et des données dont dispose l'administration et des conditions de leur mise à disposition respectivement de leur consultation, le tout en conformité avec le [RGPD] ainsi qu'avec la Directive (UE) du parlement européen et du conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public transposée par la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public »*[349].

6. La CNPD n'ayant pas été saisie directement afin d'aviser ces textes, celle-ci souhaite néanmoins s'autosaisir et se prononcer sur lesdits projets alors qu'il ressort manifestement de ce qui précède que des problématiques relevant du domaine de la protection des données à caractère personnel y sont abordées. Dans la mesure où le projet de loi et le projet de règlement grand-ducal sont connexes, la Commission nationale commentera ensemble ces deux textes dans le présent avis.

IV. Sur le projet de loi

A. Ad article 2

7. Tel que soulevé dans son avis relatif au projet de loi n°8086, la CNPD a d'ores et déjà regretté que le texte du projet de loi n°8086 ne reflète pas expressément que l'administration du cadastre et de la topographie (ci-après l' « ACT ») est à qualifier de responsable du traitement en ce qui concerne les traitements de données personnelles effectués dans le cadre de la tenue du registre national des bâtiments et des logements[350].

[348] V exposé des motifs.
[349] V exposé des motifs.
[350] Délibération n°36/AV22/2023 du 19 mai 2023 de la Commission nationale, doc. parl. n°8086/06.

8. Ainsi, il y a lieu de réitérer ses observations selon lesquelles elle avait souligné que *« la notion de responsable du traitement joue un rôle important dans l'application du RGPD dans la mesure où elle détermine qui est responsable des différentes règles en matière de protection des données ainsi que la manière dont les personnes concernées peuvent exercer leurs droits. La Commission nationale estime nécessaire que les auteurs clarifient les rôles des différents intervenants, tout en veillant à utiliser les notions et concepts existant en droit de la protection des données »*[351].

9. La Commission nationale suggère de compléter l'article 2, 8° du texte en projet en ces termes *« la gestion du registre national des bâtiments et des logements, **en sa qualité de responsable du traitement** »*.

B. Ad article 3

10. L'article 3.2 du projet de loi entérine le principe de « publicité foncière ». De telles dispositions sont nouvelles et ne figurent pas dans la loi modifiée du 25 juillet 2002 portant réorganisation de l'administration du cadastre et de la topographie, qui vise à être abrogée par le texte en projet. Il convient de féliciter les auteurs du projet de loi pour avoir consacré dans la loi un tel principe.

11. Il ressort de l'exposé des motifs que *« [l]e principe de « publicité foncière » qui permet au public de s'informer de la situation juridique d'un immeuble et comprenant d'une part des informations relatives au cadastre foncier et d'autre part la publicité hypothécaire, est repris dans le présent projet de loi afin d'expliquer l'objectif de la consultation et de la diffusion des données du registre foncier ».*

12. Les auteurs du projet de loi expliquent, en outre, qu'un tel objectif *« réside dans l'application du principe de la publicité foncière au moyen du « système informatique de la publicité foncière »*. Ce système, dont les fonctionnalités ne sont pas détaillées, serait géré par le Centre des technologies de l'information de l'État et intègrerait *« des données fournies par les notaires, l'Administration de l'enregistrement, des domaines et de la TVA et de l'Administration du cadastre et de la topographie »*. La CNPD n'est, dès lors, pas en mesure d'apprécier si un tel système serait conforme à la protection des données.

13. Il est encore précisé que l'ACT transmettrait aux tiers intéressés *« des fichiers immobiliers relatifs à la situation juridique des immeubles, sous forme d'extrait du registre foncier au moyen du système informatique de la publicité foncière. Le règlement grand-ducal détermine le degré des informations transmises dépendant de la qualité du demandeur » et que cette transmission « se fait dans la limite des informations dont dispose l'administration et dans le respect des principes qui découlent des règles »* en matière de protection des données. La CNPD reviendra infra sur les dispositions du projet de règlement grand-ducal qui visent à encadrer le principe de la communication de données à des tiers intéressés.

[351] Délibération n°36/AV22/2023 du 19 mai 2023 de la Commission nationale, doc. parl. n°8086/06, point 23, page 8.

ANNEXES

14. Par ailleurs, la Commission nationale se rallie aux observations formulées par le Conseil d'État notamment en ce qui concerne ses développements relatifs aux éléments essentiels devant figurer dans la loi. En effet, ce dernier a souligné que :

« l'article 31 de la Constitution, qui figure dans la section consacrée aux libertés publiques, dispose que : « [t]oute 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 », tandis que l'article 37 de la Constitution précise, dans sa première phrase, que « [t]oute limitation à l'exercice des libertés publiques doit être prévue par la loi et respecter leur contenu essentiel ».

Il s'ajoute à ce rappel des textes fondamentaux que la Cour constitutionnelle, en affinant sa jurisprudence antérieure, a, dans son arrêt n°177 du 3 mars 2023, retenu que « [d]'après l'article 32, paragraphe 32, de la Constitution, dans les matières réservées par la Constitution à la loi, la fixation des objectifs des mesures d'exécution doit être clairement énoncée, de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi ».

Il y a lieu de déterminer, dans l'ordre juridique national, les conditions dans lesquelles les données à caractère personnel peuvent être traitées pour une finalité autre que celle pour laquelle elles ont été collectées au sens de l'article 6, paragraphe 4, 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, ce qui couvre les hypothèses dans lesquelles des données sont communiquées par une administration à des tiers. Cette communication de données à caractère personnel à des tiers doit être strictement encadrée, ceci en application du droit à la sécurité et la confidentialité découlant du règlement européen précité.

Afin d'assurer la conformité de la disposition sous examen aux articles 31 et 37 de la Constitution, il convient, sous peine d'opposition formelle, de compléter cette disposition en précisant notamment la nature des données à caractère personnel communiquées à des tiers, la qualité du « tiers intéressé dûment identifié », ainsi que la finalité et les conditions dans lesquelles cet échange a lieu »[352].

15. Dès lors, la CNPD considère qu'il est impératif que les catégories de données qui seraient communiquées soient précisées à l'article 3 du projet de loi.

À ce titre, il est suggéré aux auteurs du projet de loi de s'inspirer des dispositions de l'article L107 A du Livre des procédures fiscales français qui dispose que *« [t]oute personne peut obtenir communication ponctuelle,*

[352] V. Avis n°61.798 du 12 juillet 2024 du Conseil d'État, doc. parl. n°8330B/2.

le cas échéant par voie électronique, d'informations relatives aux immeubles situés sur le territoire d'une commune déterminée, ou d'un arrondissement pour la Ville de Paris et les communes de Lyon et Marseille, sur lesquels une personne désignée dans la demande dispose d'un droit réel immobilier. Toute personne peut obtenir, dans les mêmes conditions, communication d'informations relatives à un immeuble déterminé. Les informations communicables sont les références cadastrales, l'adresse ou, le cas échéant, les autres éléments d'identification cadastrale des immeubles, la contenance cadastrale de la parcelle, la valeur locative cadastrale des immeubles, ainsi que les noms et adresses des titulaires de droits sur ces immeubles. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, définit les modalités d'application du présent article et les conditions de communication par voie électronique des informations visées à la phrase précédente ».

16. Elle estime que les finalités d'une telle communication de données seraient, d'après ledit article, afin *« de faire connaître aux intéressés la situation juridique d'un immeuble ».* Ces dispositions semblent implicitement viser le principe de « publicité foncière ». Toutefois pour une meilleure compréhension du texte, la CNPD se demande s'il ne serait pas opportun de définir ce principe expressément dans la loi.

V. <u>Sur le projet de règlement grand-ducal</u>

A. Ad article 2

17. L'article 2 dispose que *« [l]'utilisateur de la documentation est responsable de l'exploitation et de toute interprétation de la documentation délivrée ou consultée ».*

18. La CNPD tient à rappeler que l'article 1.4 de la loi du 29 novembre 2021 sur les données ouvertes et la réutilisation des informations du secteur public, ainsi que l'article 1.4 de la directive (UE) 2019/2024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, précisent que leurs dispositions sont notamment sans préjudice des règles relatives à la protection des données.

Le considérant 52 de ladite directive énonce que *« [l]a présente directive 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 règlement (UE) 2016/679 et la directive 2002/58/CE du Parlement européen et du Conseil, mais aussi et y compris de toute disposition de droit national complémentaire. Cela signifie, entre autres, 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 règlement (UE) 2016/679 est respecté ».*

19. Dès lors, la mise à disposition au public par l'ACT, des données visées par les textes en projet, en vertu du principe de « publicité foncière », n'implique aucunement que la réutilisation de telles données par des tiers soit, automatiquement licite et légitime au sens des articles 5 et 6 du RGPD du seul fait que ces données soient considérées comme « publiques ».

ANNEXES

En effet, sans remettre en question le principe de « publicité foncière » (même si le principe n'est pas défini dans la loi), une vigilance particulière devrait être apportée quant à la licéité des traitements effectués par les professionnels du secteur immobilier à des fins de prospection commerciale. De tels traitements ne seraient licites que si les articles 5 et 6 du RGPD sont respectés.

B. Ad article 4

20. Il y a lieu de féliciter les auteurs du projet de règlement grand-ducal pour avoir précisé les destinataires.

21. L'article 4.2 du projet de règlement grand-ducal prévoit que la délivrance d'extraits du registre foncier peut se faire « à tout intéressé identifié dans les limites de dix demandes par mois civil ».

22. À ce sujet, les auteurs du projet de règlement grand-ducal précisent que ces nouvelles dispositions entendent limiter *« cette demande à dix parcelles ou dix lots de copropriété par demande et dans une limite de dix demandes par mois civil, tel qu'inspiré par la législation française en la matière, plus précisément le décret n°2012-59 du 18 janvier 2012 relatif à la délivrance au public de certaines informations cadastrales. Cette limitation a comme objet de préserver la vie privée des personnes tout en garantissant le principe de la publicité foncière. L'identification des demandeurs, nécessaire à la vérification de la recevabilité des demandes, se fait au moyen d'une pièce d'identité »*[353].

23. Il convient de saluer l'introduction de telles dispositions qui pourraient permettre de limiter les abus en ce qui concerne la communication de données.

24. De plus, il y a plus particulièrement lieu de rendre attentifs les auteurs du projet de règlement grand-ducal à l'interprétation de l'article 15.1.c) du RGPD, qui confère à la personne concernée le droit d'obtenir du responsable du traitement des informations sur les destinataires ou catégories de destinataires auxquels les données personnelles ont été communiquées, suite à l'arrêt de la Cour de justice de l'Union européenne (ci-après la « CJUE ») du 12 janvier 2023[354].

Dans cet arrêt, la CJUE a considéré que l'article 15.1.c) du RGPD *« doit être interprété en ce sens que : le droit d'accès de la personne concernée aux données à caractère personnel la concernant, prévu par cette disposition, implique, lorsque ces données ont été ou seront communiquées à des destinataires,* ***l'obligation pour le responsable du traitement de fournir à cette personne l'identité même de ces destinataires, à moins qu'il ne soit impossible d'identifier ces destinataires*** *ou que ledit responsable du traitement ne démontre que les demandes d'accès de la personne concernée sont manifestement infondées ou excessives, au sens de l'article 12, paragraphe 5, du règlement 2016/679,*

[353] V. commentaire des articles sous Ad 4.
[354] CJUE, arrêt du 12 janvier 2023, RW c. Österreichische Post AG, C-154/21, ECLI:EU:C:2023:3, point 52.

auxquels cas celui-ci peut indiquer à cette personne uniquement les catégories de destinataires en cause » (souligné en gras).

25. Or, en l'absence d'un système d'authentification forte des personnes à l'origine de la demande de délivrance d'un extrait du registre foncier, l'ACT ne pourra faire droit à la demande des personnes concernées sur base de l'article 15.1.c) du RGPD en ce qui concerne les personnes ayant demandé un extrait du registre foncier concernant la propriété des personnes concernées. S'il ressort du commentaire des articles que *« l'identification des demandeurs, nécessaire à la vérification de la recevabilité des demandes, se fait au moyen d'une pièce d'identité »*, la Commission nationale se demande si une telle solution serait transposable aux demandes par voie électronique, ainsi qu'aux demandes émanant des personnes morales[355].

26. Ainsi, il y a lieu de regretter que les modalités concrètes d'un tel mécanisme ne soient pas précisées dans le texte en projet. En ce qui concerne la communication des données par l'ACT par voie électronique, la CNPD suppose que celle-ci reposera sur la procédure actuelle qui permet la communication d'extraits de documentation cadastrale sur le site geoportail.lu via un compte utilisateur[356]. Si la Commission nationale comprend que l'identification des personnes physiques se ferait au moyen d'une carte d'identité[357], les modalités d'un tel contrôle dans le cadre d'une communication par voie électronique ne sont pas précisées. En outre, qu'en est-il des moyens d'identification des personnes morales ?

En tout état de cause, la Commission nationale estime indispensable la mise en place d'un système d'authentification forte des personnes à l'origine de la demande de délivrance d'un extrait de la documentation cadastrale.

27. A toutes fins utiles, en ce qui concerne les modalités de la communication des informations prévues à l'article 4.2.1° précité, la CNPD se permet de renvoyer aux dispositions réglementaires précisées à l'article R°107 A-6 du Livre des procédures fiscales français qui entend prévoir que *« [l]a communication des informations susmentionnées est réalisée, si le demandeur en a fait le choix, par voie électronique à l'exclusion de tout autre moyen. Dans ce cas, elle a lieu par courrier électronique si le demandeur a fourni une adresse électronique et valide ou dans le cadre d'une application informatique à accès contrôlée dotée d'une traçabilité et dont le responsable a satisfait aux formalités préalables du chapitre IV de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés »*. Il est ainsi suggéré aux auteurs du projet de règlement grand-ducal de s'en inspirer.

C. Ad article 6

28. L'article 6 entend prévoir *« des droits d'accès en ligne d'une partie ou l'intégralité*

[355] V. supra point 23.
[356] V. https://extraits.geoportail.lu/?lang=fr.
[357] V. commentaires des articles sous Ad 4.

ANNEXES

du registre foncier » aux entités énumérées audit article. Ces dispositions reprennent les dispositions de l'article 9 du règlement grand-ducal du 10 août 2018, ayant vocation à être abrogé par le texte sous examen.

29. Dans la mesure où un accès direct au registre foncier est prévu, il convient de rappeler que le responsable du traitement se doit de respecter le principe d'intégrité et confidentialité visé à l'article 5.1.f) du RGPD. Par ailleurs, 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.

30. Il y a lieu de rappeler qu'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 l'entité concernée, et à quelles données précises cette personne ou ce service aurait accès.

31. 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.

32. Par ailleurs, la Commission nationale souligne l'importance d'effectuer proactivement des contrôles en interne. À cet effet, il convient conformément à l'article 32.1.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 ».*

33. Enfin, la CNPD se demande quelles seraient les mesures mises en place par l'ACD pour s'assurer du respect des dispositions de l'article 4.2.1° du projet de règlement grand-ducal qui prévoit que « tout intéressé identifié » puisse obtenir un extrait du registre foncier « dans la limite de dix demandes par mois civil ».

En effet, dans l'hypothèse où des salariés d'une même société obtiendraient individuellement la délivrance d'extraits du registre foncier, ce cas d'espèce ne constituerait-il pas un détournement des quotas fixés par l'article précité ?

Ainsi adopté à Belvaux
en date du 7 août 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

6

Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 8082 sur l'impôt foncier, l'impôt à la mobilisation de terrains et l'impôt sur la non-occupation de logements, modifiant 1° la loi modifiée dite « Abgabenordnung (AO) » du 22 mai 1931 ; 2° la loi modifiée dite « Bewertungsgesetz (BewG) » du 16 octobre 1934 ; 3° la loi modifiée dite « Steueranpassungsgesetz (StAnpG) » du 16 octobre 1934 ; 4° la loi modifiée du 17 avril 1964 portant réorganisation de l'administration des contributions directes ; 5° la loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu ; 6° la loi modifiée du 30 avril 2004 autorisant le Fonds national de solidarité à participer aux prix des prestations fournies dans le cadre de l'accueil aux personnes admises dans un centre intégré pour personnes âgées, une maison de soins ou un autre établissement médico-social assurant un accueil de jour et de nuit ; 7° la loi modifiée du 19 juillet 2004 concernant l'aménagement communal et le développement urbain ; 8° la loi modifiée du 22 octobre 2008 sur le droit d'emphytéose et le droit de superficie et introduisant différentes mesures administratives et fiscales en faveur de la promotion de l'habitat ; 9° la loi modifiée du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement ; 10° la loi du 28 juillet 2018 relative au revenu d'inclusion sociale ; 11° la loi du 22 juillet 2022 relative à une subvention de loyer et abrogeant : 1° la loi modifiée du 19 juillet 1904 sur les impositions communales ; 2° la loi modifiée dite « Grundsteuergesetz (GrStG) » du 1er décembre 1936

Délibération n°52/AV20/2024
du 7 août 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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* ».

L'article 36.4 du RGPD dispose que « *[l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement.* »

2. N'ayant pas été saisie directement par le Ministère de l'Intérieur, la Commission nationale souhaite néanmoins se prononcer sur le projet de loi n° 8082 sur l'impôt foncier, l'impôt à la mobilisation de terrains et l'impôt sur la non-occupation de logements, modifiant 1° la loi modifiée dite « Abgabenordnung (AO) » du 22 mai 1931 ; 2° la loi modifiée dite « Bewertungsgesetz

ANNEXES

(BewG) » du 16 octobre 1934 ; 3° la loi modifiée dite « Steueranpassungsgesetz (StAnpG) » du 16 octobre 1934 ; 4° la loi modifiée du 17 avril 1964 portant réorganisation de l'administration des contributions directes ; 5° la loi modifiée du 4 décembre 1967 concernant l'impôt sur le revenu ; 6° la loi modifiée du 30 avril 2004 autorisant le Fonds national de solidarité à participer aux prix des prestations fournies dans le cadre de l'accueil aux personnes admises dans un centre intégré pour personnes âgées, une maison de soins ou un autre établissement médico-social assurant un accueil de jour et de nuit ; 7° la loi modifiée du 19 juillet 2004 concernant l'aménagement communal et le développement urbain ; 8° la loi modifiée du 22 octobre 2008 sur le droit d'emphytéose et le droit de superficie et introduisant différentes mesures administratives et fiscales en faveur de la promotion de l'habitat ; 9° la loi modifiée du 23 décembre 2016 concernant la collecte, la saisie et le contrôle des dossiers d'aides relatives au logement ; 10° la loi du 28 juillet 2018 relative au revenu d'inclusion sociale ; 11° la loi du 22 juillet 2022 relative à une subvention de loyer et abrogeant : 1° la loi modifiée du 19 juillet 1904 sur les impositions communales ; 2° la loi modifiée dite « Grundsteuergesetz (GrStG) » du 1er décembre 1936 (ci-après le « projet de loi »).

3. La Commission nationale tient à relever que si la fiche d'évaluation d'impact du projet de loi indique qu'elle aurait été consultée avant son dépôt, tel n'a pas été le cas.

Dans son avis sur le projet de loi n°8086 relative aux registres national et communaux des bâtiments et des logements[358], la CNPD a d'ailleurs regretté de ne pas avoir été saisie pour avis lors du dépôt du projet de loi actuellement sous examen alors que ce dernier prévoit notamment l'interconnexion du registre national des bâtiments et des logements, dont la création est prévue par le projet de loi n°8086, avec le registre national des personnes physiques (ci-après le « RNPP »).

4. Il ressort de l'exposé des motifs que l'un des objectifs principaux du projet de loi sous avis est de lutter contre la pénurie de logements en introduisant des impôts visant, d'une part, à inciter les propriétaires à mobiliser leurs terrains et, d'autre part, à (faire) occuper des logements vacants.

5. Afin de pouvoir identifier les objets imposables, le projet de loi entend créer des nouveaux registres, tels que le registre national des fonds non construits ou le registre des logements non-occupés. Étant donné que les informations figurant dans ces registres se rapportent à une ou plusieurs personne(s) physique(s) identifiée(s) ou identifiable(s), à savoir le(s) propriétaire(s), elles sont à considérer comme des données à caractère personnel[359] dont le traitement est soumis au RGPD. Le présent avis limitera ses observations aux aspects du projet de loi ayant trait à la protection des données à caractère personnel.

[358] Délibération n°36/AV22/2023 du 19 mai 2023 de la Commission nationale pour la protection des données, doc. parl. n°8086/07.
[359] Au sens de l'article 4.1) du RGPD.

XXVIII. Remarques liminaires

6. Il ressort de l'exposé des motifs que le projet de loi *« vise à concilier deux objectifs principaux, qui tiennent à la réforme de l'impôt foncier et à la lutte contre la pénurie de logements ». « Ainsi, le projet de loi porte sur trois types d'impositions différentes qui s'inscrivent dans une suite logique, consistant dans une imposition par couches superposées »*[360].

7. Afin de remédier à la pénurie de logements dont souffre le Luxembourg, le projet de loi prévoit notamment la création de deux nouveaux instruments fiscaux, à savoir l'impôt à la mobilisation de terrains et l'impôt à la non-occupation de logements.

8. Ainsi, l'article 2 du projet de loi précise que le ministre est compétent pour fixer la valeur de base et pour établir le bulletin de valeur de base.

Les dispositions dudit article répartissent ensuite les compétences au niveau de la fixation, du prélèvement et du recouvrement de ces impôts entre les communes (pour l'impôt foncier) et l'ACD (pour l'impôt à la mobilisation de terrains).

Ces impôts impliquent des traitements de données personnelles qui constituent une ingérence au droit à la protection de la vie privée et au droit à la protection des données à caractère personnel, tels que consacrés notamment par les articles 20 et 31 de la Constitution ainsi que les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

9. Les droits au respect de la vie privée et à la protection des données personnelles ne sont toutefois pas des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société et être mis en balance avec d'autres droits fondamentaux[361].

10. À cet égard, il est à noter que la Constitution érige le droit au logement en objectif à valeur constitutionnelle[362]. Conformément aux articles 37 de la Constitution et 52.1 de la Charte, des limitations peuvent être apportées aux droits au respect à la vie privée et à la protection des données personnelles, pourvu qu'elles soient prévues par la loi, qui doit être formulée avec une précision suffisante[363], et respectent le contenu essentiel des droits fondamentaux ainsi que le principe de proportionnalité. La Cour européenne des droits de l'Homme souligne aussi régulièrement qu'une ingérence au droit au respect de la vie privée n'est prévue par la loi que si la disposition légale est prévisible[364].

XXIX. L'accès au RNPP et au registre communal des personnes physiques

11. Plusieurs dispositions du projet de loi accordent à certaines autorités le pouvoir

[360] V. exposé des motifs point II.3.2., page 71 du projet de loi.
[361] CJUE, arrêt du 7 mars 2024, Endemol Shine Finland Oy, C-740/22, ECLI:EU:C:2024:216, point 52.
[362] Art. 40 de la Constitution : L'État veille à ce que toute personne puisse vivre dignement et disposer d'un logement approprié.
[363] CJUE, arrêt du 8 avril 2014, Digital Rights Ireland Ltd, C-293/12 et C-594/12, ECLI:EU:C:2014:238, point 54.
[364] Pour un examen plus approfondi, v. : Délibération n° 3/AV3/2021 du 20 février 2021 de la Commission nationale pour la protection des données, doc. parl. n° 7691/03, point II.2A.

ANNEXES

de consulter le RNPP ainsi que le registre communal des personnes physiques.

12. Ainsi, il résulte de l'article 7.2 du projet de loi que le ministre ayant l'Intérieur dans ses attributions (ci-après le « ministre »), le receveur communal et l'Administration des contributions directes (ci-après l' « ACD ») sont habilités à consulter le RNPP pour déterminer la résidence habituelle du contribuable dans le contexte des notifications.

13. L'article 26.1, alinéa 2, dispose que le collège des bourgmestre et échevins est autorisé à accéder au registre communal des personnes physiques ou, au besoin, au RNPP afin d'identifier les bénéficiaires de l'abattement forfaitaire sur l'impôt foncier. L'article 33.2, alinéa 2, prévoit encore que l'ACD est habilitée à accéder au RNPP pour identifier les enfants du contribuable donnant, le cas échéant, lieu à l'abattement forfaitaire.

14. La CNPD se rallie aux observations du Conseil d'État relatives aux articles 7 et 26 selon lesquelles ces dispositions peuvent être omises. En effet, la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques ainsi que le règlement grand-ducal du 28 novembre 2013 fixant les modalités d'application de la loi du 19 juin 2013 relative à l'identification des personnes physiques définissent les modalités d'accès au RNPP.

XXX. Les traitements de données personnelles afférentes à la valeur de base

15. L'article 2 du projet de loi précise que le ministre est compétent pour fixer la valeur de base et pour établir le bulletin de valeur de base. Cet article indique encore que la valeur de base ainsi déterminée sert de base au calcul à l'impôt foncier ainsi qu'à l'impôt à la mobilisation de terrains[365]. Dès lors, et afin de fixer la valeur de base pour établir le bulletin de valeur de base, le ministre est amené à collecter des données à caractère personnel.

Une fois la valeur de base déterminée par le ministre, ce dernier met à disposition, conformément à l'article 15 du projet de loi, les données visées aux articles 13.1er, 13.6, et 21 du projet de loi, au collège des bourgmestre et échevins ainsi qu'à l'ACD. Ces données permettent ainsi de fixer, prélever et recouvrir l'impôt foncier pour le collège des bourgmestre et échevins ainsi que pour l'ACD en ce qui concerne l'impôt à la mobilisation de terrains.

A. Le(s) responsable(s) du traitement

16. Tout d'abord, il y a lieu de rappeler que la notion de responsable du traitement joue un rôle capital dans l'application du RGPD dans la mesure où elle détermine qui est responsable du respect des différentes règles en matière de protection des données ainsi que la manière dont les personnes concernées peuvent exercer leurs droits[366]. Dès lors, il est important de pouvoir identifier correctement quelle entité est responsable du traitement.

[365] V. section 2 du projet de loi, articles 10 à 16.
[366] V. en ce sens: Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 3., disponibles sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr.

17. L'article 16.1 du projet de loi dispose que *« le ministre a la qualité de responsable du traitement des données afférentes à la valeur de base ».* La CNPD comprend ainsi que le ministre serait le responsable du traitement en ce qui concerne les traitements de données liés à la fixation de la valeur de base.

B. Les finalités des traitements

18. Il convient de relever que la notion de « finalité », c'est-à-dire l'objectif poursuivi par le traitement, occupe une place primordiale au sein du RGPD. Aux termes de l'article 5.1.b) du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

De plus, d'autres principes prévus par le RGPD, tels que les principes de minimisation des données[367] ou de limitation de conservation[368] s'apprécient au regard des finalités pour lesquelles les données sont traitées. Par conséquent, il est important que les finalités soient clairement définies dans le projet de loi.

19. L'article 16.2, première phrase, du projet de loi énumère de manière limitative les finalités pour lesquelles les données afférentes à la valeur de base peuvent être traitées, à savoir la fixation, le prélèvement et le recouvrement de l'impôt foncier et de l'impôt à la mobilisation de terrains.

20. Par ailleurs, la deuxième phrase de l'article 16.2 précisent que les données afférentes à la valeur de base *« peuvent également être traitées pour des finalités scientifiques, statistiques, administratives et fiscales, à condition que la finalité de ces traitements soit compatible avec les finalités pour lesquelles les données ont été établies et collectées ».*

21. Dans son avis du 13 juin 2023, le Conseil d'État estime, en renvoyant à l'article 89 du RGPD, que la deuxième phrase du paragraphe 2 est superflue[369]. La CNPD peut souscrire dans une certaine mesure à l'analyse du Conseil d'État.

Cependant, elle tient à rappeler que le traitement ultérieur à des fins de recherche scientifique et à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales, à condition d'être soumis, conformément à l'article 89.1 du RGPD, à des garanties appropriées pour les droits et libertés de la personne concernée.

La pseudonymisation, voire l'anonymisation, sont mises en avant par l'article 89.1 du RGPD comme des mesures permettant de garantir les droits et libertés des personnes concernées. Or, en cas d'accès direct à l'intégralité des données figurant dans le registre des logements non-occupés, le ministre ayant le Logement dans ses attributions aurait accès à des informations qui peuvent être attribuées directement à une personne physique, à savoir le contribuable, et qui ne sont dès lors pas pseudonymisées, voire anonymisées.

[367] Article 5.1.c) du RGPD
[368] Article 5.1.e) du RGPD
[369] Avis 61.195 du Conseil d'État du 13 juin 2023, doc. parl. n° 8082/05, p. 13.

ANNEXES

Il est également rappelé que l'article 65 de la loi précitée du 1er août 2018 doit être respecté dans le cadre des traitements de données mis en œuvre à des fins statistiques ou à des fins de recherche scientifique.

22. Enfin, il convient de souligner que les articles précités ainsi que l'article 89 du RGPD ne s'appliquent qu'aux traitements à des fins de recherche scientifique ou historique ou à des fins statistiques. Dès lors, en ce qui concerne les finalités administratives et fiscales évoquées par la disposition sous examen, la Commission nationale estime que les termes utilisés sont beaucoup trop vagues et ne permettent pas de savoir quelle utilisation concrète serait faite des données afférentes à la valeur de base.

C. Les catégories de données figurant sur le bulletin de valeur de base

23. L'article 13.1 du projet de loi énumère limitativement les informations figurant sur le bulletin de valeur de base, établi par le ministre, et qui seraient par la suite mises à disposition des autorités chargées de la fixation, du prélèvement et du recouvrement respectivement de l'impôt foncier ou de l'impôt à la mobilisation de terrains.

24. Or, l'article 13.6 du projet de loi dispose que *« [l]e contenu du bulletin de valeur de base énoncé au paragraphe 1er peut être complété par toute autre mention utile ».* La CNPD regrette un tel ajout et estime qu'en application des articles 31 et 37 de la Constitution, les données que le ministre serait amené à mettre à disposition d'autres autorités devraient être limitativement énoncées au niveau de la loi[370].

D. La mise à disposition des données des bulletins de valeur de base

25. L'article 15 du projet de loi a trait à la mise à disposition des données des bulletins de valeur de base au collège des bourgmestre et échevins ainsi qu'à l'ACD afin que ces derniers puissent fixer respectivement l'impôt foncier et l'impôt à la mobilisation de terrains.

26. Bien que l'article précité reste muet quant à la manière dont cette mise à disposition s'opère, il résulte du commentaire des articles qu'il s'agirait d'un accès direct par voie électronique. À l'instar du Syndicat des villes et communes luxembourgeoises (ci-après le « Syvicol »)[371], la CNPD considère qu'il convient de le préciser dans le texte proprement dit du projet de loi.

27. Il convient de s'interroger sur les modalités de la communication des données, visée à l'article 15 alinéa 2 du projet de loi : la communication se fera-t-elle par le biais d'un accès au registre national des fonds non construits ? Si tel devait être le cas, pour une meilleure lisibilité des dispositions, cet accès devrait être précisé à l'article 22 du projet loi. En effet, cet article entend encadrer l'accès audit registre.

En tout état de cause, des clarifications à ce sujet mériteraient d'être apportées par les auteurs du projet de loi.

[370] V. en ce sens : Avis 60.868 du Conseil d'État du 22 décembre 2023, doc. parl. n° 7932/05, p. 7.
[371] Avis du Syvicol du 33 mai 2023, doc. parl. n° 8082/03, p. 11.

XXXI. Le registre national des fonds non construits

28. La loi en projet prévoit la création d'un registre national des fonds non construits en vue de l'établissement de l'impôt à la mobilisation de terrains.

A. Le(s) responsable(s) du traitement

29. L'article 24 du projet de loi dispose que *« [l]e ministre, respectivement le bourgmestre, ont la qualité de responsables du traitement des données dans le cadre de l'établissement du registre [...] ».*

Au vu de l'importance de la notion du responsable du traitement dans l'application du RGPD[372], cette disposition soulève les interrogations suivantes : s'agit-il d'une responsabilité conjointe ou de responsables du traitement indépendants et successifs qui interviennent à des stades différents de la chaîne d'opérations de traitement ? S'il devait s'agir de responsabilité conjointe, l'article 26 du RGPD serait applicable. Une clarification du texte à ce sujet s'impose.

30. À toutes fins utiles, la CNPD rappelle que la notion de responsable du traitement est un concept fonctionnel en ce qu'il vise à répartir les responsabilités en fonction des rôles réels des parties[373]. Cela implique que la désignation en tant que responsable du traitement par le projet de loi devrait concorder avec les activités réellement effectuées par l'entité en question.

Si la qualification du ministre en tant que responsable du traitement semble correspondre aux tâches qui lui sont confiées par la loi en projet, des doutes subsistent quant à la qualification du bourgmestre. Tout comme le Syvicol[374], la Commission nationale note à cet égard le caractère limité du rôle accordé au bourgmestre dans le cadre du registre national des fonds non construits.

Selon le commentaire des articles, *« la plupart du temps, l'intervention du bourgmestre consiste à informer le ministre du fait que le gros œuvre sur un chantier a été achevé, de manière à ce que le fonds en question ne saurait plus être qualifié de fonds non construit [...]. Le contrôle à effectuer par le bourgmestre porte dès lors uniquement sur les fonds non construits sur lesquels des travaux de construction ont été entamés depuis la dernière mise à jour du registre ».*

B. Les finalités du traitement

31. Bien que l'article 24 du projet de loi soit intitulé « Responsabilités et finalités du traitement des données », l'article se borne à déterminer quelle entité est à qualifier de responsable du traitement et ne contient aucune indication quant aux finalités poursuivies par les traitements effectués par le biais du registre national des fonds non construits.

[372] Point 16 du présent avis.
[373] Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, point 12, disponibles sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en.
[374] Avis du Syvicol du 33 mai 2023, doc. parl. n° 8082/03, p. 14.

ANNEXES

32. L'article 17 du projet de loi précise toutefois les objectifs du registre national des fonds non construits. Ainsi, ce registre répond notamment à des besoins fiscaux, administratifs, statistiques et scientifiques. En ce qui concerne les traitements à des fins statistiques et scientifiques, la CNPD se permet de renvoyer à ses développements formulés aux points 21 et 22 du présent avis.

33. L'article 17.2 du projet de loi précise encore que *« [l]e registre a pour finalité de répertorier au niveau national les fonds non construits, les fonds viabilisés et les fonds non viabilisés, en vue de l'établissement du bulletin de valeur de base et du bulletin de l'impôt à la mobilisation de terrains de ces fonds ».*

34. Ainsi, pour une meilleure compréhension du texte sous avis, de telles précisions devraient figurer à l'article 24 du projet de loi, qui a pour objet dans son intitulé « les finalités du traitement des données ».

C. L'accès au registre national des fonds non construits

35. L'article 22.1 du projet de loi prévoit que le bourgmestre dispose d'un accès au registre national des fonds non construits afin qu'il puisse informer le ministre des « adaptations » à effectuer conformément à l'article 19.3.

36. Selon l'article 22.2 du projet de loi, le notaire et les autorités, amenés à constituer une emphytéose ou un droit de superficie, auraient accès au registre pour informer les personnes concernées du fait que l'impôt à la mobilisation de terrains est, le cas échéant, susceptible d'être exigible. Comme soulevé précédemment pour l'article 15[375], il pourrait être utile de préciser qu'il s'agit d'un accès direct par voie électronique.

37. L'article 22.3 du projet de loi dispose encore que toute autre personne aurait accès au registre dans les formes prévues par l'article 23. L'article 22.4 dispose que l'Administration du cadastre et de la topographie assure qu'une visualisation du registre sous forme d'une carte interactive serait publiquement accessible sur le site du Géoportail.

38. La CNPD suppose que toutes les données énumérées à l'article 21 du projet de loi seraient comprises dans cette carte et regrette que les auteurs ne se prononcent pas sur les raisons les ayant conduit à prévoir la création d'une telle carte publiquement accessible.

Ces derniers indiquent, dans le commentaire des articles, simplement que *« par principe, le registre est public, afin que les mutations immobilières puissent être effectuées en connaissance de cause d'un éventuel impôt à la mobilisation de terrains susceptible d'être exigible »*. Les auteurs du projet de loi ont-ils voulu faire un parallèle avec l'accès à la documentation cadastrale qui est accessible au public, sous certaines conditions, en vertu du principe de « publicité foncière »[376] ? Ainsi, la Commission

[375] Point 18 du présent avis.
[376] V. Article 3 du projet de loi n°8330B.

nationale se trouve dans l'impossibilité de se prononcer sur la proportionnalité de ce traitement de données.

39. Par ailleurs, de telles dispositions soulèvent les questions suivantes : comment les dispositions de l'article 22.3 du projet de loi s'articulent-elles avec les dispositions de la loi du 26 juillet 2010 portant transposition de la directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE) en droit national ? Plus particulièrement les restrictions d'accès prévues à l'article 11 de la loi du 29 juillet 2010 précitée pourraient-elles s'appliquer en l'espèce ?

D. Les extraits

40. Il ressort de l'article 23 du projet de loi, lu ensemble avec l'article 22.3, que toute personne peut demander un extrait du registre des fonds non construits comportant les mentions prévues par l'article 21.

La demande et l'extrait sont établis sous forme électronique et par l'intermédiaire du site du Géoportail. Ici encore, les auteurs du projet de loi restent muets quant aux raisons pour lesquelles toute personne, sans devoir justifier d'un intérêt particulier, est en droit de recevoir un tel extrait, de sorte que la CNPD ne peut apprécier la proportionnalité de cette mesure.

Comme relevé ci-avant au point 38, elle se demande si les auteurs du projet de loi ont voulu établir un parallèle avec l'accessibilité de la documentation cadastrale en vertu du principe de « publicité foncière ».

Toutefois, il y a lieu de relever que l'article 4 du projet de règlement grand-ducal (élaboré en parallèle du Projet de loi 8330B) concernant la consultation et la diffusion de la documentation relative à la mensuration officielle, de la documentation cadastrale, de la documentation topographique, du registre national des localités et des rues et des systèmes de référence de coordonnées nationaux gérés par l'Administration du cadastre et de la topographie ; et portant fixation du tarif des redevances 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, entend encadrer, voir limiter, sous certaines conditions, la délivrance d'extraits.

Il y a lieu de regretter que pareilles mesures ne sont aucunement prévues par le projet de loi sous avis.

41. La Commission nationale se permet encore d'attirer l'attention des auteurs du projet de loi sur les remarques relevées par le Conseil d'État quant à l'article 3 du projet de loi n°8330B selon lesquelles il a estimé que :

« Cet article fournit la base légale à un règlement grand-ducal pour la consultation et la diffusion de la documentation relative à la mensuration officielle, de la documentation cadastrale, de la documentation topographique, du registre national des localités et des rues et des systèmes de référence de coordonnées nationaux gérés par l'Administration. Le Conseil d'État se trouve actuellement saisi d'un projet de règlement grand-ducal correspondant qui porte également fixation

ANNEXES

du tarif des redevances à percevoir au profit de l'État pour les travaux de bureau et de terrain exécutés par l'Administration, en vertu de l'article 14, paragraphe 1er, du projet de loi sous revue.

En ce qui concerne la nature des données à consulter par des tiers, le Conseil d'État note qu'il s'agit de données à caractère personnel et rappelle, à cet égard, que l'article 31 de la Constitution, qui figure dans la section consacrée aux libertés publiques, dispose que « [t]oute 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 », tandis que l'article 37 de la Constitution précise, dans sa première phrase, que « [t]oute limitation à l'exercice des libertés publiques doit être prévue par la loi et respecter leur contenu essentiel ».

Il s'ajoute à ce rappel des textes fondamentaux que la Cour constitutionnelle, en affinant sa jurisprudence antérieure, a, dans son arrêt n° 177 du 3 mars 2023, retenu que « [d]'après l'article 32, paragraphe 32, de la Constitution, dans les matières réservées par la Constitution à la loi, la fixation des objectifs des mesures d'exécution doit être clairement énoncée, de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi ».

Il y a lieu de déterminer, dans l'ordre juridique national, les conditions dans lesquelles les données à caractère personnel peuvent être traitées pour une finalité autre que celle pour laquelle elles ont été collectées au sens de l'article 6, paragraphe 4, 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, ce qui couvre les hypothèses dans lesquelles des données sont communiquées par une administration à des tiers. Cette communication de données à caractère personnel à des tiers doit être strictement encadrée, ceci en application du droit à la sécurité et la confidentialité découlant du règlement européen précité.

Afin d'assurer la conformité de la disposition sous examen aux articles 31 et 37 de la Constitution, il convient, sous peine d'opposition formelle, de compléter cette disposition en précisant notamment la nature des données à caractère personnel communiquées à des tiers, la qualité du « tiers intéressé dûment identifié », ainsi que la finalité et les conditions dans lesquelles cet échange a lieu »[377].

42. Force est de constater que le projet de loi sous examen ne précise pas les modalités de délivrance de ces extraits. La Commission nationale recommande fortement aux

[377] V. Avis n°61.798 du 12 juillet 2024 du Conseil d'État, doc. parl. n°8330B/2.

auteurs du projet de loi de prévoir les modalités de délivrance de tels extraits à l'instar du projet de règlement grand-ducal concernant la consultation et la diffusion de la documentation relative à la mensuration officielle, de la documentation cadastrale, de la documentation topographique, du registre national des localités et des rues et des systèmes de référence de coordonnées nationaux gérés par l'Administration d cadastre et de la topographie ; et portant fixation du tarif des redevances 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, qui entend encadrer, voir limiter, sous certaines conditions, la délivrance d'extraits.

43. Par ailleurs, il y a plus particulièrement lieu de rendre attentifs les auteurs du projet de loi à l'interprétation de l'article 15.1.c) du RGPD, qui confère à la personne concernée le droit d'obtenir du responsable du traitement des informations sur les destinataires ou catégories de destinataires auxquels les données personnelles ont été communiquées, suite à l'arrêt de la Cour de justice de l'Union européenne (ci-après la « CJUE ») du 12 janvier 2023[378].

Dans cet arrêt, la CJUE a considéré que l'article 15.1.c) du RGPD *« doit être interprété en ce sens que : le droit d'accès de la personne concernée aux données à caractère personnel la concernant, prévu par cette disposition, implique, lorsque ces données ont été ou seront communiquées à des destinataires, **l'obligation pour le responsable du traitement de fournir à cette personne l'identité même de ces destinataires**, à moins qu'il ne soit impossible d'identifier ces destinataires ou que ledit responsable du traitement ne démontre que les demandes d'accès de la personne concernée sont manifestement infondées ou excessives, au sens de l'article 12, paragraphe 5, du règlement 2016/679, auxquels cas celui-ci peut indiquer à cette personne uniquement les catégories de destinataires en cause »* (souligné en gras).

44. La Commission nationale est d'avis que pour se conformer à cet arrêt, le(s) responsable(s) du traitement, devrai(en)t mettre en place un système d'authentification forte des personnes à l'origine de la demande de délivrance d'un extrait de la documentation cadastrale, ce qui permettrait une plus grande transparence vis-à-vis des propriétaires concernés. Ces derniers ont en effet le droit, sur base de l'article 15.1.c) du RGPD, d'obtenir du ou des responsable(s) du traitement des informations sur les personnes ayant obtenu un extrait relatif à leur propriété.

E. Les mesures de sécurité

45. Enfin, dans la mesure où un accès au registre des logements non-occupés est prévu par le texte en projet, il convient de rappeler que le responsable du traitement se doit de respecter le principe d'intégrité et confidentialité visé à l'article 5.1.f) du RGPD. L'article 32 du RGPD dispose encore que *« le responsable du traitement et le sous-traitant*

[378] CJUE, arrêt du 12 janvier 2023, RW c. Österreichische Post AG, C-154/21, ECLI:EU:C:2023:3, point 52.

ANNEXES

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.

Il y a lieu de rappeler qu'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 l'entité concernée, 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.

Finalement, la Commission nationale souligne l'importance d'effectuer proactivement des contrôles en interne. À cet effet, il convient conformément à l'article 32.1.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 ».*

XXXII. Les traitements de données afférentes à l'impôt foncier

46. Les articles du Chapitre 2 du projet de loi sous examen traitent de l'impôt foncier.

L'article 31, intitulé « Responsabilités et finalités du traitement des données », énonce dans son paragraphe 1er que *« [l]e collège des bourgmestre et échevins, respectivement le receveur communal ont la qualité de responsable du traitement des données afférentes à l'impôt foncier à partir du délai prévu à l'article 15 [...] »*, donc à partir de la mise à disposition, par le ministre, des données des bulletins de valeur de base.

47. L'article 31.2 du projet de loi indique de manière limitative les finalités du traitements des données afférentes à l'impôt à la mobilisation des terrains d'un fonds non construit en disposant qu'elles *« ne peuvent être traitées pour des finalités autres que la fixation, le prélèvement et le recouvrement de l'impôt en vue duquel les données ont été générées ».*

La deuxième phrase précise que ces données *« peuvent également être traitées pour des finalités scientifiques, statistiques, administratives et fiscales, à condition que la finalité de ces traitements soit compatible avec les finalités pour lesquelles les données ont été établies et collectées »*. Il est renvoyé aux développements sous les points 21 et 22 du présent avis.

XXXIII. Les traitements de données afférentes à l'impôt à la mobilisation de terrains

48. L'article 40 du projet de loi se prononce sur la responsabilité ainsi que les finalités du traitement des données. Le paragraphe 1er indique que le directeur de l'ACD a la qualité de responsable du traitement des données afférentes à l'impôt à la mobilisation de

terrains à partir du délai prévu à l'article 16. La CNPD suppose qu'il s'agit d'une erreur matérielle et que les auteurs visent en réalité le délai prévu à l'article 15, alinéa 2, c'est-à-dire à partir de la mise à disposition, par le ministre, des données des bulletins de valeur de base.

49. Pour ce qui est des finalités énumérées à l'article 40.2 du projet de loi, la CNPD estime que l'article 40.2, deuxième phrase, est rédigé en des termes trop imprécis pour permettre de savoir quelle utilisation concrète sera faite de ces données[379].

XXXIV. Le registre des logements non-occupés

50. Dans le cadre de l'introduction d'un impôt sur la non-occupation de logements, le projet de loi prévoit la création d'un registre des logements non-occupés, ayant pour but d'identifier les logements susceptibles de faire l'objet de cet impôt. Cette identification permettant par la suite l'établissement du bulletin de l'impôt sur la non-occupation de logements.

51. S'il y a lieu de saluer que le principe même de la tenue d'un registre soit inscrit dans le projet de loi, certains points mériteraient d'être détaillés avec plus de précision.

A. Le(s) responsable(s) du traitement

52. En vertu de l'article 43.3, le bourgmestre et l'ACD sont à qualifier de responsable du traitement en ce qui concerne les traitements mis en œuvre à travers le registre sous examen.

Ainsi, selon l'article 43.3, premier alinéa 1er du projet de loi, le bourgmestre a la qualité de responsable du traitement. Le deuxième alinéa dispose encore que *« [s]ans préjudice des dispositions de l'alinéa 1er, à partir de la mise à disposition de données prévue par l'article 45, le directeur de l'Administration des contributions directes a la qualité de responsable du traitement des données afférentes au constat de l'état de non-occupation d'un logement qui le concernent, dans les conditions de l'alinéa 1er ».*

La CNPD comprend que le bourgmestre a la qualité de responsable du traitement pour les traitements de données à des fins d'identification des logements non-occupés. En outre, il ressort également du commentaire des articles que le bourgmestre assurerait une gestion courante dudit registre.

53. L'ACD, serait quant à elle, selon la compréhension de la CNPD, responsable du traitement de données à des fins d'établissement de l'impôt sur la non-occupation de logements.

Or, il convient de relever que l'article 55 du projet de loi désigne le directeur de l'ACD en tant que responsable du traitement des données afférentes à l'impôt sur la non-occupation de logements. La Commission nationale se demande si ces dispositions sont nécessaires alors qu'elles semblent

[379] Points 21 et 22 du présent avis.

ANNEXES

réitérer les dispositions de l'article 43.3 du projet de loi.

À toutes fins utiles, il convient de relever que l'article 55 s'intitule « responsabilité des données ». La CNPD suggère d'omettre ces termes et de les remplacer par la notion de « responsable du traitement », telle que définie par l'article 4.7 du RGPD.

54. Par ailleurs, il convient de relever que les auteurs du projet de loi précisent dans le commentaire des articles qu' *« au niveau communal, le bourgmestre est le responsable du traitement des données à caractère personnel. Au niveau national, cette responsabilité revient au directeur de l'Administration des contributions directes »*.

Ainsi, l'architecture même du registre des logements non-occupés interroge : s'agit-il d'un registre national unique ou chaque commune dispose-t-elle de son propre registre au niveau communal ? Le système du registre des logements non-occupés ne fonctionnerait-il pas comme le registre national, tel que visé à l'article 3 de la loi relative à l'identification des personnes physiques, qui est alimenté par les registres communaux, visés à l'article 17 de ladite loi ? Si tel devait être le cas, les auteurs du projet de loi pourrait s'inspirer des dispositions précitées.

En tout état de cause, pour une meilleure compréhension du fonctionnement dudit registre des clarifications mériteraient d'être apportées par les auteurs du projet de loi.

55. Enfin, dans l'hypothèse où il s'agirait d'un registre national unique, il y aurait également lieu de clarifier la relation entre les différents responsables du traitement que sont les bourgmestres, en tant que représentants des différentes administrations communales.

Sont-ils des responsables conjoints au sens de l'article 26 du RGPD ou, en revanche, des responsables indépendants ? Par ailleurs, il importerait d'assurer que chaque commune n'ait accès qu'aux informations relatives aux logements relevant de leur compétence territoriale, conformément au principe de minimisation des données[380].

56. En tout état de cause, pour une meilleure lisibilité des dispositions sous avis et dans la mesure où le registre poursuit plusieurs finalités pour des traitements effectués par plusieurs responsables du traitement, il conviendrait de préciser séparément pour chacun des traitements poursuivant l'une des finalités énoncées à l'article 43 du projet de loi qui en est le responsable du traitement.

B. Les finalités du traitement

57. L'article 43.2 du projet de loi dispose que *« [l]es finalités du traitement des données au registre des logements non-occupés sont l'identification des logements non-occupés, ainsi que la gestion de l'impôt sur la non-*

[380] Article 5.1.c) du RGPD.

occupation de logements au niveau national. [...] ».

Le troisième paragraphe, dernier alinéa, précise encore que *« [l]es données afférentes au constat de l'état de non-occupation d'un logement ne peuvent être employées à des finalités autres que la fixation, le prélèvement et le recouvrement de l'impôt sur la non-occupation de logements, ainsi qu'à des finalités statistiques et de recherche scientifique. »* Sur ce point, il est renvoyé aux développements formulés sous les points 21 et 22 du présent avis.

C. L'accès au registre des logements non-occupés

58. L'article 43.4 du projet de loi prévoit que le ministre ayant le Logement dans ses attributions a accès au registre des logements non-occupés pour des finalités statistiques et de recherche scientifique. Si les auteurs du projet de loi envisagent un accès direct par voie électronique, il conviendrait de le préciser dans le texte du projet de loi afin de renforcer la sécurité juridique.

59. De plus, il ressort de l'article 45 du projet de loi que le bourgmestre met à la disposition de l'ACD les décisions du constat de l'état de non-occupation d'un logement. Si cette disposition reste, de nouveau, muette quant à la manière dont cette mise à disposition s'opère, l'ACD aurait, en vertu de l'article 51.1 du projet de loi, accès au registre des logements non-occupés pour ce faire. Ainsi, ne faudrait-il pas prévoir cet accès à l'article 43 plutôt que de le prévoir à l'article 51 ?

En outre, la Commission nationale suppose qu'il s'agit d'un accès direct par voie électronique. Il serait toutefois préférable, pour des raisons de sécurité juridique, que cette précision se trouve dans le texte du projet de loi.

60. Enfin, dans la mesure où un accès au registre des logements non-occupés est prévu par le texte en projet, il convient de rappeler que le responsable du traitement se doit de respecter le principe d'intégrité et confidentialité visé à l'article 5.1.f) du RGPD. 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.

Il y a lieu de rappeler qu'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 l'entité concernée, 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.

Finalement, la Commission nationale souligne l'importance d'effectuer

ANNEXES

proactivement des contrôles en interne. À cet effet, il convient conformément à l'article 32.1.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 ».*

D. L'interconnexion

61. En vertu de l'article 43.5 du projet de loi, *« [d]ans les limites des informations prévues au paragraphe 1er, le registre des logements non-occupés est interconnecté au registre national des bâtiments et des logements, au registre national des personnes physiques et à la documentation cadastrale ».*

Il résulte de l'article 44.1 du projet de loi que l'état de non-occupation d'un logement est constaté par le bourgmestre, après interconnexion du registre national des bâtiments et des logements et du RNPP. Ni le texte du projet de loi, ni le commentaire des articles ne donnent d'indications sur les caractéristiques de cette interconnexion ou sur les données au sein des différents fichiers qui feraient l'objet de cette interconnexion.

À l'exception de l'interconnexion du registre national des bâtiments et des logements et du RNPP qui a pour objectif de constater l'état de non-occupation d'un logement, le texte sous examen reste par ailleurs muet sur les finalités poursuivies par les différentes interconnexions.

62. À cet égard, la CNPD donne à considérer que la mise en relation automatisée d'informations provenant de fichiers distincts et ayant des finalités différentes est susceptible de constituer une ingérence importante au droit à l'autodétermination informationnelle ainsi qu'au droit à la protection des données personnelles.

Une telle ingérence relève des matières réservées à la loi en vertu des articles 31 et 37 de la Constitution, de sorte que les contours de cette interconnexion devraient être détaillés de manière précise dans le texte de loi, ce qui n'est actuellement pas le cas.

63. Par ailleurs, se pose la question de savoir si le principe de minimisation des données est en l'espèce respecté. Aux termes de l'article 5.1.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.

Le projet de loi sous examen prévoit l'interconnexion de plusieurs registres, dont notamment le RNPP, qui contient un grand nombre d'informations fournissant une vue très détaillée sur les aspects relevant de la vie privée des personnes physiques, et le registre national des bâtiments et des logements, pour lequel il n'est pas clair quelles catégories de données auraient vocation à y figurer[381].

La CNPD déplore que les auteurs du projet de loi ne fournissent pas d'explications quant aux raisons rendant nécessaire une telle interconnexion et se demande si des moyen moins intrusifs, tel qu'un simple accès aux

[381] Délibération n°36/AV22/2023 du 19 mai 2023 de la Commission nationale pour la protection des données, doc. parl. n° 8086/07, point 20.

différents registres, permettent d'atteindre les finalités poursuivies, qui, à l'exception de la détection des logements non-occupés, ne ressortent d'ailleurs pas clairement du projet de loi sous examen.

64. Il y a également lieu de se demander si l'interconnexion des différents registres, telle que prévue par le projet de loi, ne permettrait pas de contourner les règles régissant leur accès.

À titre d'exemple, les modalités d'accès au RNPP sont déterminées par la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques ainsi que par le règlement grand-ducal du 28 novembre 2013 fixant ses modalités d'application. Il devrait être veillé à ce que l'interconnexion ne confère pas un accès à des organismes ou personnes qui n'auraient pas reçu un tel accès en application des règles régissant le registre en question.

65. Finalement, la Commission nationale se rallie à l'avis du Syvicol[382] en ce qu'il constate que l'identificateur introduit par le projet de loi n° 8086 n'est pas mentionné à l'article 43 du projet de loi qui énumère les données figurant au registre des logements non-occupés.

Or, ce sera cet identificateur qui permettra l'interconnexion des différents registres. Les auteurs du projet de loi devraient veiller à énumérer de manière exhaustive toutes les données figurant dans le registre des logements non-occupés.

[382] Avis du Syvicol du 33 mai 2023, doc. parl. n° 8082/03, p. 17.

E. La présomption de non-occupation

66. L'article 44 de la loi en projet introduit des présomptions de non-occupation d'un logement. Le premier paragraphe prévoit une présomption pouvant être constatée automatiquement par voie informatisée, et plus précisément en interconnectant le registre national des bâtiments et des logements et le RNPP. Il est renvoyé aux développements sous les points 61 à 65 du présent avis.

67. Le paragraphe 2 énonce encore d'autres présomptions de non-occupation, comme l'hypothèse où la consommation de services en eau potable ou en énergie constatée pendant une période d'au moins six mois consécutifs est inférieure à une consommation minimale.

La CNPD s'interroge sur la manière dont ces présomptions seraient constatées par le bourgmestre. Par quels moyens le bourgmestre constatera-t-il que la consommation de services en énergie d'un ménage aura été inférieure inférieur à une consommation minimale pendant six mois consécutifs ?

Si la fourniture en eau potable est assurée par la commune, tel n'est pas le cas pour la fourniture en énergie. Dans le cas où cette disposition nécessiterait un échange de données personnelles entre le bourgmestre et le fournisseur d'énergie, il devrait être prévu expressément par la loi, ce que le projet de loi ne fait pourtant pas.

ANNEXES

En outre, en vertu du principe de proportionnalité, des limitations au droit à la protection des données personnelles ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt généraux. Le commentaire des articles évoque ce principe mais n'explique pas pourquoi les auteurs estiment qu'il serait respecté en l'espèce. Face au manque de précision du texte quant à la manière dont le bourgmestre pourrait vérifier la consommation en énergie des ménages, la CNPD se trouve dans l'impossibilité de se prononcer sur la proportionnalité.

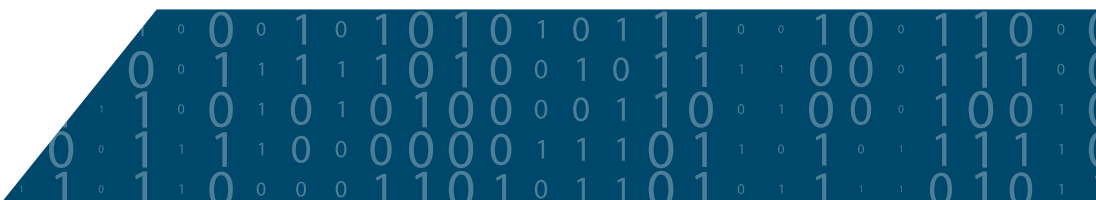
Ainsi adopté à Belvaux
en date du 7 août 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire



Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8186A portant modification de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; de la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes, des droits d'accise sur l'eau-de-vie et des cotisations d'assurance sociale ; de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines, de l'Administration des douanes et accises et portant modification de la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée; la loi générale des impôts (« Abgabenordnung ») ; la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes ; la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines ; la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale

Délibération n°53/AV21/2024
du 7 août 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après la « Commission nationale » ou la « CNPD ») « *conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ».

2. Par ailleurs, l'article 36.4 du RGPD dispose que « *[l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement.* ».

3. Par courrier en date du 28 mars 2023, Madame la Ministre des Finances a invité la Commission nationale à se prononcer sur le projet de loi portant modification de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; de la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes, des droits d'accise sur l'eau-de-vie et des cotisations d'assurance sociale ; de la loi modifiée du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif ; de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines, de l'Administration des douanes et accises et portant modification de la loi

ANNEXES

modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée ; la loi générale des impôts (« Abgabenordnung ») ; la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes ; la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines; la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale.

4. Il ressort de l'exposé des motifs que le projet de loi a notamment pour objectif de modifier la loi générale des impôts (ci-après « AO ») et certaines lois connexes dans une optique de simplification et de modernisation des procédures applicables aux contribuables. Le projet de loi tient encore à élargir le transfert des informations dans le cadre de la coopération interadministrative afin de permettre à l'Administration des contributions directes (ci-après « l'ACD ») d'échanger des renseignements nécessaires à l'exercice de leurs missions respectives tant avec la Commission de surveillance du secteur financier (ci-après la « CSSF ») qu'avec le Commissariat aux assurances (ci-après le « CAA »).

5. La Commission des Finances, lors de sa réunion du 17 juillet 2024, a décidé de scinder le projet de loi précité en deux projets de loi distincts :

- Le projet de loi 8186A portant modification 1° de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; 2° de la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes, des droits d'accise sur l'eau-de-vie et des cotisations d'assurance sociale ; 3° de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines, de l'Administration des douanes et accises et portant modification de - la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée; la loi générale des impôts (« Abgabenordnung ») ; la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes ; la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines ; la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale (ci-après le « projet de loi ») ; et
- Le projet de loi 8186B portant modification 1° de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; 2° de la loi modifiée du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif.

6. En parallèle, la Commission nationale a été saisie de quatre projets de règlements grand-ducaux élaborés dans le contexte des dispositions modifiées ou introduites par le projet de loi[383]. Après analyse des

[383] Projet de règlement grand-ducal portant exécution de l'alinéa 4 du paragraphe 171 de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; Projet de règlement grand-ducal portant exécution de l'article 12a de la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes, des droits d'accise sur l'eau-de-vie et des cotisations d'assurance sociale ; Projet de règlement grand-ducal portant exécution de l'alinéa 2 du paragraphe 22bis de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; Projet de règlement grand-ducal portant exécution du paragraphe 29c de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung »).

projets de règlements grand-ducaux lui soumis, la CNPD n'a pas pu identifier de questions relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement de données à caractère personnel. Elle n'estime donc pas nécessaire de se prononcer sur les projets de règlements grand-ducaux susmentionnés. Dès lors, le présent avis limitera ses observations aux questions traitant les aspects du projet de loi portant sur la protection des données dans le cadre du projet de loi.

I. <u>Quant à l'article 1er du projet de loi</u>

7. L'article 1er du projet de loi a pour objet d'introduire un nouvel article §22bis *« afin de permettre à l'ACD de déléguer certaines fonctions informatiques pour les informations qui devront être divulguées au prestataire de ces services »*[384]. Ces dispositions prévoient une dérogation ponctuelle au respect du secret fiscal.

8. De plus, selon le commentaire des articles, la finalité de cette nouvelle disposition est d'étendre la violation des dispositions du §22 AO à des personnes externes à l'ACD dans le cadre de l'exécution de travaux spécifiques ou de leur sous-traitance. Ainsi, le projet de loi prévoit que l'ACD est autorisée à confier l'exécution de travaux ponctuels à des contractants et aux sous-traitants. Les dispositions du secret fiscal s'appliquent dans ce cas aux prestataires de ces services.

9. Il convient encore de préciser que le paragraphe 3 du nouvel article §22bis dispose que *« [l]orsque, pour les besoins de l'exécution des travaux visés aux alinéas 1er ou 2, une prise de connaissance des informations couvertes par le secret fiscal, au sens du §22, s'avère nécessaire, l'accès à ces informations ne peut être effectué que sur autorisation préalable du directeur de l'Administration des contributions directes ou de son délégué »*. Le paragraphe 4 de l'article précité dispose, en outre, que *« [t]oute révélation des informations couvertes par le secret fiscal, dont une personne a pris connaissance selon les termes énoncés à l'alinéa 3, qui est effectuée en dehors de l'exécution des travaux visés aux alinéas 1er ou 2, est sanctionnée conformément au §412 ».*

10. Il y a lieu de féliciter les auteurs du projet de loi d'avoir prévu de telles dispositions alors que les informations couvertes par le secret fiscal pourraient comprendre des données à caractère personnel.

11. En outre, selon la compréhension de la Commission nationale, le CTIE agirait en tant que sous-traitant de l'ACD[385]. Il y a lieu de rappeler que l'article 4.8 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 »*. Il convient de souligner que le traitement de données à caractère personnel effectué par

[384] Avis n°61.390 du Conseil d'État du 11 juillet 2023, doc. parl. n°8186/04, p. 3.
[385] V. en ce sens: Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 3., disponibles sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr

ANNEXES

le CTIE pour le compte de l'ACD doit être régi par un contrat ou un autre acte juridique conformément à l'article 28 du RGPD. Enfin, 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, des fuites de données ou des modifications non désirées.

II. Quant à l'article 3 du projet de loi

A. Remarques liminaires

12. L'article 3 du projet de loi sous avis modifie la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines et de l'Administration des douanes et accises (ci-après la « loi modifiée du 19 décembre 2008 »), en insérant deux nouveaux chapitres pour permettre des échanges réciproques d'informations entre l'ACD et la CSSF[386], ou l'ACD et le CAA[387].

13. Tout d'abord, il y a lieu de rappeler que le RGPD n'aura vocation à s'appliquer que si l'échange, tel que prévu par le projet de loi, implique un traitement de données à caractère personnel. L'article 3 du RGPD définit comme données à caractère personnel *« 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 ».*

14. De plus, le considérant 14 du RGPD énonce que *« [l]e présent règlement 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 ».* Cependant, des informations ayant trait à des personnes morales peuvent, le cas échéant, concerner des personnes physiques et dès lors être considérées comme des données à caractère personnel. En effet, le groupe de travail « Article 29 »[388] dans son avis 4/2007 sur le concept de données à caractère personnel du 20 juin 2007, WP 136, indique que « les informations ayant trait à des personnes morales peuvent également être considérées comme *« concernant » des personnes physiques en tant que telles (...). Cela peut être le cas lorsque le nom de la*

[386] Nouveau chapitre IVbis.
[387] Nouveau chapitre IVter.
[388] Le groupe de travail « article 29 » était un organe consultatif qui conseillait la Commission sur les questions de protection des données et qui a contribué à l'élaboration de politiques harmonisées en matière de protection des données dans l'UE. Après l'entrée en application du RGPD le 25 mai 2018, le comité européen de la protection des données a succédé à ce groupe de travail.

personne morale est dérivé de celui d'une personne physique. Un autre cas de figure est celui du courrier électronique d'une entreprise qui est normalement utilisé par un employé, ou des informations concernant une petite entreprise (du point de vue juridique, un « objet » plutôt qu'une personne morale) qui peuvent éventuellement décrire le comportement de leur propriétaire ».

15. En outre, la Commission Européenne précise également dans ses *« [l]ignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne »*, dans quel cas des données relatives à des personnes morales sont susceptibles de constituer des données à caractère personnel[389].

B. Sur le traitement ultérieur des données à caractère personnel pour une finalité différente

16. Conformément à l'article 5.1.b) du RGPD, les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

17. Cependant, le considérant 50 du RGPD énonce que *« [l]e traitement de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement ne devrait être autorisé que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement. Dans ce cas, aucune base juridique distincte de celle qui a permis la collecte des données à caractère personnel n'est requise. Si 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, le droit de l'Union ou le droit d'un État membre peut déterminer et préciser les missions et les finalités pour lesquelles le traitement ultérieur devrait être considéré comme compatible et licite. (...) La base juridique prévue par le droit de l'Union ou le droit d'un État membre en ce qui concerne le traitement de données à caractère personnel peut également constituer la base juridique pour un traitement ultérieur. Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres: de tout lien entre ces finalités et les finalités du traitement ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement, quant à l'utilisation ultérieure desdites données; la nature des données à caractère personnel; les conséquences pour les personnes concernées du traitement ultérieur prévu; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu ».*

[389] Communication de la Commission au Parlement européen et au Conseil du 29 mai 2019, « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », COM (2019) 250 final.

ANNEXES

18. L'article 6.4 du RGPD précise les conditions à respecter dans le cadre d'un traitement à une fin autre que celle pour laquelle les données ont été collectées et dispose que *« [l]orsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1, le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres :*

a. de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé;
b. du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement;
c. de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10;
d. des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées;
e. de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation ».

19. Il y a lieu de relever que dans son avis relatif au projet de loi n°7872, le Conseil d'État a relevé que « la condition de licéité du traitement prévue à l'article 6, paragraphe 1, lit. e) du RGPD ne concerne que la collecte et le traitement initial de données personnelles par les autorités publiques. Or, dans la mesure où, dans le cadre du projet sous avis, des données à caractère personnel seront transférées à une autorité publique autre que le responsable du traitement initial pour une finalité différente de celle pour laquelle ces données ont été collectées, cette autorité devra vérifier les conditions alternatives de l'article 6, paragraphe 4, du RGPD qui permettent le traitement ultérieur des données. Le transfert des données entre autorités publiques peut être légitime si le traitement ultérieur est fondé sur une disposition légale qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des objectifs visés à l'article 23, paragraphe 1, du RGPD. Le projet sous avis vise à créer cette base légale nécessaire au traitement ultérieur de données pour une finalité différente de celle pour laquelle ces données ont été collectées et le Conseil d'État vérifiera dans le cadre de l'examen des articles si les dispositions sous avis poursuivent un but énuméré à l'article 23, paragraphe 1, du RGPD et si le traitement envisagé est proportionné par rapport à ce but »[390].

[390] V. Avis n°60.741 du Conseil d'État du 1er février 2022, doc. parl. n° 7872/04, p.2.

20. Par ailleurs, le Conseil d'État a souligné, dans son avis relatif au texte sous examen, que l'établissement correct de l'impôt constitue un intérêt public légitime, tout comme la bonne marche du contrôle prudentiel ainsi que la lutte contre le blanchiment de capitaux et la lutte contre le financement du terrorisme[391]. La Commission nationale se rallie à l'avis du Conseil d'État et considère que cette finalité *« constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés l'article 23 [du RGPD] »*[392].

21. En effet, l'article 23.1.e) du RGPD dispose que *« [l]e droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir : (...) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale »*.

22. De plus, il convient encore de relever que la Cour de Justice de l'Union européenne a reconnu que *« contribuer à la lutte contre la fraude et l'évasion fiscales internationales [...] constitue un objectif d'intérêt général reconnu par l'Union »*[393]. Il y a, dès lors, lieu de féliciter les auteurs du projet de loi d'avoir établi une base légale pour le traitement ultérieur de données personnelles pour une finalité différente de celle pour laquelle ces données ont été initialement collectées.

23. Finalement, il faut souligner que lorsqu'une restriction aux droits des personnes est prévue par une mesure législative, celle-ci doit inclure des dispositions spécifiques concernant les informations énumérées à l'article 23.2 du RGPD. Ainsi, le projet de loi devrait contenir des dispositions précises relatives aux finalités ou catégories de traitement, aux catégories de données à caractère personnel, à l'étendue des limitations introduites, aux garanties visant à prévenir les abus ou les accès et transferts illicites, à la détermination du responsable du traitement, aux durées de conservation, aux risques pour les droits et libertés des personnes concernées et au droit de celles-ci d'être informées de la limitation. La CNPD constate néanmoins que le projet de loi omet de prendre en compte les dispositions obligatoires énoncées au paragraphe 2 de l'article 23 du RGPD, qui précise les éléments que toute mesure législative fondée sur l'article 23.1 doit inclure.

[391] V. Avis n°61.390 du Conseil d'État du 11 juillet 2023, doc. parl. n° 8186/04, p.14.
[392] Article 6.4 du RGPD.
[393] CJUE, C-245/19 et C-246/19, État luxembourgeois, 6 octobre 2020, § 86-87.

ANNEXES

C. Quant à l'échange de données entre l'ACD et la CSSF

24. L'article 3 du projet de loi introduit un nouvel article 16bis dans la loi modifiée du 19 décembre 2008 dont les nouvelles dispositions prévoient un échange de données entre l'ACD et la CSSF « sur demandes motivées respectives » qui porterait sur les *« renseignements, actes et documents en leur possession qui concernent des contribuables qui sont des entités soumises à la surveillance prudentielle de la Commission de surveillance du secteur financier ou pour lesquelles la Commission de surveillance du secteur financier est l'autorité compétente pour assurer le respect des obligations professionnelles en matière de lutte contre le blanchiment et le financement du terrorisme »*[394].

25. Le paragraphe 2 dudit article 16bis prévoit quant à lui que *« les renseignements, actes et documents transmis par la Commission de surveillance du secteur financier à l'Administration des contributions directes en vertu du paragraphe 1er doivent être nécessaires dans le cadre de l'exécution de la législation en matière de divers impôts directs ou de l'exercice des attributions et perceptions confiées à l'Administration des contributions directes par les dispositions légales spéciales ».*

26. L'article 16bis.3 prévoit encore que *« les renseignements, actes et documents transmis par l'Administration des contributions directes à la Commission de surveillance du secteur financier en vertu du paragraphe 1er doivent être nécessaires pour l'exercice de la surveillance prudentielle exercée par la Commission de surveillance du secteur financier ou pour assurer le respect par les entités visées au paragraphe 1er de leurs obligations professionnelles en matière de lutte contre le blanchiment et le financement du terrorisme ».*

27. La Commission nationale note que le premier paragraphe de l'article 16bis précise les modalités de l'échange des données ainsi que les personnes concernées par ce traitement. Elle salue particulièrement le fait que cet échange de données se fasse uniquement sur demande motivée, ce qui exclut un échange automatique de données.

Les deuxième et troisième paragraphes énoncent les finalités respectives de la transmission des données. À ce sujet, les auteurs du projet de loi précisent dans le commentaire de l'article 3 (nouvel article 16bis) que *« [l]a coopération entre l'ACD et la CSSF est nécessaire pour éviter qu'un contribuable qui est en même temps un établissement surveillé par la CSSF en tant qu'autorité prudentielle ou pour lequel la CSSF contrôle le respect des obligations professionnelles en matière d'AML/FT puisse faire des déclarations incohérentes ou contradictoires à la CSSF respectivement à l'ACD ».* La Commission nationale comprend donc que la finalité poursuivie par le transfert de données entre l'ACD et la CSSF serait d'assurer que les contribuables, qui sont en même temps des entités soumises à la surveillance de la CSSF, émettent des déclarations cohérentes à l'égard de

[394] Nouvel article 16bis.1 introduit par l'article 3 du projet de loi.

l'administration fiscale ou à l'égard de la CSSF.

28. L'article 3 du projet de loi introduit également un article 16ter qui prévoit de nouvelles communications de données entre l'ACD et la CSSF. Le premier paragraphe de l'article 16ter énumère la finalité de la transmission à savoir *« de vérifier que les institutions financières déclarantes luxembourgeoises n'adoptent pas de pratiques ayant pour but de contourner la communication d'informations prévue par la loi modifiée du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) et la loi modifiée du 24 juillet 2015 relative à FATCA ». En outre, il ressort du commentaire de l'article que « les renseignements, actes et documents échangés [...] ont uniquement trait à d'éventuelles pratiques ayant pour but de contourner la communication d'informations prévue par la loi modifiée du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) et la loi modifiée du 24 juillet 2015 relative à FATCA. La mise en place de cet échange d'information n'a pas pour objectif de vérifier la conformité fiscale des clients des institutions financières concernées »*. La CNPD se félicite que les auteurs du projet de loi aient précisé les finalités pour lesquelles les données seraient transmises.

29. Néanmoins, la Commission nationale constate que dans le cadre de l'article 16ter, l'échange de données ne se fait pas sur demande motivée comme prévu par l'article 16bis.1 et s'interroge sur les raisons pour lesquelles les auteurs du projet de loi ont décidé d'omettre cette précision. Elle suggère fortement de l'ajouter également dans l'article 16ter étant donné que le texte sous avis entend déroger aux dispositions de la loi modifiée du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) et la loi modifiée du 24 juillet 2015 relative à FATCA qui disposent que les données doivent être utilisées uniquement pour les finalités prévues dans ces lois[395].

30. Enfin, bien que les traitements envisagés par les dispositions sous examen soient fondés sur une disposition légale qui constitue une mesure nécessaire et proportionnée dans une société démocratique, le principe de minimisation des données consacré à l'article 5.1.c) du RGPD selon lequel les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, devra également être respecté.

D. Quant à l'échange de données entre l'ACD et le CAA

31. L'échange des données entre l'ACD et le CAA est introduit par l'article 17bis dans la loi modifiée du 19 décembre 2008, qui prévoit dans son premier paragraphe que *« sur demandes motivées respectives, l'Administration des contributions directes et le Commissariat aux Assurances échangent les renseignements, actes et documents en leur possession qui concernent des contribuables qui sont des entités soumises à*

[395] V. Art. 6.1 de la loi modifiée du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) et art. 4.1 de la loi modifiée du 24 juillet 2015 relative à FATCA.

ANNEXES

la surveillance prudentielle du Commissariat aux Assurances ou pour lesquelles le Commissariat aux Assurances est l'autorité compétente pour assurer le respect des obligations professionnelles en matière de lutte contre le blanchiment et le financement du terrorisme ».

32. Le paragraphe 2 dudit article 17bis prévoit quant à lui que *« les renseignements, actes et documents transmis par la Commissariat aux Assurances à l'Administration des contributions directes en vertu du paragraphe 1er doivent être nécessaires dans le cadre de l'exécution de la législation en matière de divers impôts directs ou de l'exercice des attributions et perceptions confiées à l'Administration des contributions directes par les dispositions légales spéciales ».*

33. L'article 17bis.3 dispose, en outre, que *« les renseignements, actes et documents transmis par l'Administration des contributions directes au Commissariat aux Assurances en vertu du paragraphe 1er doivent être nécessaires pour l'exercice de la surveillance prudentielle exercée par le Commissariat aux Assurances ou pour assurer le respect par les entités visées au paragraphe 1er de leurs obligations professionnelles en matière de lutte contre le blanchiment et le financement du terrorisme ».*

34. Le projet de loi introduit également un article 17ter qui prévoit la transmission des informations recueillies par le CAA *« dans le cadre de ses missions légales et susceptibles d'être utiles aux fins de vérifier que les institutions financières déclarantes luxembourgeoises n'adoptent pas de pratiques ayant pour but de contourner la communication d'informations prévue par la loi modifiée du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) et la loi modifiée du 24 juillet 2015 relative à FATCA »* à l'ACD.

35. La CNPD note que les dispositions concernant la coopération entre l'ACD et le CAA sont axées sur les dispositions des articles 16bis et 16ter relatives à la coopération entre l'ACD et la CSSF et réitère ses observations formulées ci-avant[396]. Elle se félicite que les auteurs du projet de loi définissent les finalités pour lesquelles les renseignements, actes et documents peuvent être transmis et rappelle que seules les données à caractère personnel qui sont nécessaires à la réalisation des finalités poursuivies par le responsable du traitement doivent être transmises (principe de minimisation des données).

E. Quant aux dérogations au secret fiscal et au secret professionnel

36. Il y a lieu de rappeler que les violations du secret professionnel sont punies par les sanctions pénales prévues à l'article 458 du Code pénal. Il en découle que les exceptions au secret doivent être prévues par la loi et qu'elles sont d'interprétation stricte. Le cadre régissant l'échange d'informations doit donc être établi par la loi afin d'assurer un niveau adéquat de sécurité juridique.

[396] Voir points 23 et s. du présent avis.

37. En l'espèce, les échanges de données prévues par l'article 3 du projet de loi sont considérés comme une dérogation au secret professionnel respectivement au secret fiscal[397].

38. Dans le commentaire des articles, les auteurs du projet de loi sous avis soulignent que *« les informations reçues par l'ACD sont toutes soumises au secret fiscal prévu au paragraphe 22 AO et les informations reçues par la CSSF sont soumises au secret professionnel visé à l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier »*[398].

39. Ainsi, les informations transmises à la CSSF ou au CAA en vertu du présent projet de loi bénéficieront d'une protection au moins équivalente à celle imposée à l'ACD, conformément à l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier respectivement l'article 7 de la loi du 7 décembre 2015 sur le secteur des assurances.

40. La CNPD se félicite, dès lors, que les auteurs du projet de loi aient prévu une dérogation au secret fiscal et au secret professionnel dans le texte de loi.

F. Sur la sécurité de l'information

41. Conformément à l'article 5.1.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 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 ».*

42. Ainsi, dans le cadre de la mise en œuvre d'échanges de données entre les différentes autorités publiques par voie informatique, ou via des procédés automatisés ou non, de telles mesures de sécurité devraient être mises en œuvre par les différents responsables du traitement 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 ou le service, au sein de chaque administration concernée et à quelles données précises cette personne ou ce service aurait accès.

43. 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.

[397] V. Article 3 du projet de loi qui introduit un article 16ter.3 et un article 17ter.3 dans la loi modifiée du 19 décembre 2008.
[398] V. Ad art. 3 (nouvel article 16bis) du projet de loi.

ANNEXES

44. Finalement, la Commission nationale souligne l'importance d'effectuer proactivement des contrôles en interne. À cet effet, il convient conformément à l'article 32.1.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 ».*

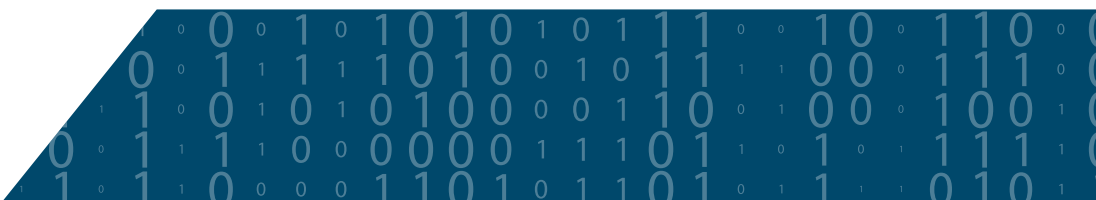
Ainsi adopté à Belvaux
en date du 7 août 2024.

La Commission nationale
pour la protection des données

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire



6

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°7650 portant modification 1° du Code de la consommation ; 2° de la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des spécialités pharmaceutiques et des médicaments préfabriqués ; 3° de la loi modifiée du 27 juillet 1991 sur les médias électroniques ; 4° de la loi modifiée du 27 juillet 1997 sur le contrat d'assurance ; 5° de la loi modifiée du 14 août 2000 relative au commerce électronique ; 6° de la loi modifiée du 24 mai 2011 relative aux services dans le marché intérieur ; 7° de la loi modifiée du 23 décembre 2016 sur les ventes en soldes et sur trottoir et la publicité trompeuse et comparative ; 8° de la loi du 26 juin 2019 relative à certaines modalités d'application et à la sanction du règlement (UE) 2018/302 du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n°2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE, en vue de la transposition de la directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE

Délibération n°54/AV22/2024
du 16 août 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. »*

2. En date du 05 mai 2023, la Commission nationale a avisé le projet de loi n°7650 portant modification 1° du Code de la consommation ; 2° de la loi modifiée du 11 avril 1983 portant réglementation de la mise sur le marché et de la publicité des spécialités pharmaceutiques et des médicaments préfabriqués ; 3° de la loi modifiée du 27 juillet 1991 sur les médias électroniques ; 4° de la loi modifiée du 27 juillet 1997 sur le contrat d'assurance ; 5° de la loi modifiée du 14 août 2000 relative

ANNEXES

au commerce électronique ; 6° de la loi modifiée du 24 mai 2011 relative aux services dans le marché intérieur ; 7° de la loi modifiée du 23 décembre 2016 sur les ventes en soldes et sur trottoir et la publicité trompeuse et comparative ; 8° de la loi du 26 juin 2019 relative à certaines modalités d'application et à la sanction du règlement (UE) 2018/302 du Parlement européen et du Conseil du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur, et modifiant les règlements (CE) n°2006/2004 et (UE) 2017/2394 et la directive 2009/22/CE, en vue de la transposition de la directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (ci-après le « projet de loi »)[399].

3. Par courrier du 29 mars 2024, Madame la Ministre de l'Agriculture, de l'Alimentation et de la Viticulture - Direction de la protection des consommateurs - a invité la Commission nationale à se prononcer sur les amendements gouvernementaux au projet de loi, qui ont été approuvés par le Conseil de gouvernement dans sa séance du 08 avril 2024 (ci-après les « amendements gouvernementaux »).

4. Il y a lieu de rappeler que le texte sous avis est destiné à transposer la directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE. Les derniers amendements gouvernementaux ont pour objectif, quant à eux, de répondre aux objections du Conseil d'État, telles que délivrées dans son dernier avis en date du 20 juin 2023 concernant plus particulièrement la procédure judiciaire, le règlement extrajudiciaire du litige collectif ou encore les titulaires de l'action, et ce afin d'assurer une transposition fidèle de la directive (UE) 2020/1828 précitée.

5. La Commission nationale limitera ses observations aux dispositions légales concernant la protection des données personnelles et aux interactions potentielles avec la procédure d'enquête formelle devant la CNPD suite à l'instruction d'une réclamation. Tout en réitérant certaines de ses observations émises dans son avis initial, elle s'interroge aussi sur certaines modifications apportées par les derniers amendements gouvernementaux.

6. A titre liminaire, la CNPD salue d'ores et déjà la correction de l'erreur matérielle quant à sa dénomination notamment au sein de l'article 6 du projet de loi et l'article L. 321-4 du Code de la consommation tels que modifiés.

I) Quant à la qualité pour agir

7. Au vu de l'article 3 des amendements gouvernementaux et l'article L.321-2 du Code de la Consommation, en lien avec le nouvel article L.321-4 du Code de la Consommation,

[399] Délibération n°34/AV20/2023 du 5 mai 2023 de la Commission nationale pour la protection des données.

tels que modifiés, la Commission nationale constate et salue le fait de pouvoir introduire, comme déjà prévu par les précédents amendements gouvernementaux du 16 septembre 2022, une action en cessation ou en interdiction après la constatation d'une violation en lien avec la réglementation sur la protection des données et notamment les dispositions du RGPD tel que listé à l'annexe 1, tout comme un recours collectif en réparation en tant qu'entité régulatrice sectorielle ainsi que rappelé par le présent projet de loi.

8. Concernant plus spécifiquement le recours collectif, le projet initial qui attribuait qualité pour agir à cinq catégories de titulaires exclut désormais cette qualité, dans sa version modifiée, au profit du consommateur individuel qui pourra seulement opter de se joindre au groupe ainsi que celle de l'attribution facultative de la qualité pour agir à des associations non agréées désignées ad hoc par le tribunal compétent. La CNPD comprend donc que les amendements sous revue maintiennent la qualité pour agir aux entités qualifiées c'est-à-dire les entités régulatrices sectorielles dont elle fait partie, les associations agréées et les entités qualifiées désignées par un État membre de l'Union européenne. L'article L.321-3 du Code de la consommation, tel que modifié, prévoit quant à lui une liste des « entités qualifiées désignées à l'avance » communiquée par chaque État membre puis publiée par la Commission européenne pour les actions et recours transfrontières et par le ministre ayant la Protection des consommateurs dans ses attributions pour les actions et recours nationaux.

9. La Commission nationale se demande donc si lesdits changements répondent à ses interrogations soulevées dans son avis initial. Pour rappel, la CNPD avait soulevé dans son précédent avis[400] l'importance que les dispositions en question prévoient bien les mêmes critères pour déterminer une entité qualifiée pouvant exercer l'action en cessation ou en interdiction ou un recours collectif que ceux énoncés par l'article 80 du RGPD et tel que d'ailleurs soutenu par le Contrôleur européen de la protection des données (ci-après le « CEPD ») dans son avis 8/2018[401]. Ainsi, comment ces deux dispositions légales prévoyant chacune des dispositions particulières pour la détermination d'une entité qualifiée s'articuleront donc entre elles en pratique ?

10. De plus, la CNPD s'interroge toujours sur le fait de savoir comment dans les faits pourrait-elle, exercer ces nouveaux pouvoirs, voire si et comment d'autres entités qualifiées, non encore concrètement déterminées, pourraient intenter une action ayant pour cause commune un manquement de même nature aux dispositions du RGPD ? En effet, 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[402] reste muette en la matière. La loi du 1er août 2018 relative

[400] Voir Délibération n°34/AV20/2023 du 5 mai 2023 de la Commission nationale pour la protection des données, point 12.
[401] Avis 8/2018, CEPD, « Une nouvelle donne pour les consommateurs », point 63.
[402] 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, Mém. A686.

ANNEXES

à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ainsi qu'en matière de sécurité nationale[403], quant à elle, prévoit dans son article 46 « représentation des personnes concernées » certaines conditions dédiées à la représentation de la personne concernée de manière générale par une personne morale. À titre comparatif, la loi organique française « Informatique et Libertés »[404] prévoit explicitement un article 37 dédié à l'action de groupe qui avait déjà été introduite en France par la loi n°2014-344 du 17 mars 2014 relative à la consommation et rappelle également les différents titulaires de cette action. La Commission nationale réitère donc à ce titre son questionnement sur la nécessité de modifier d'un point de vue légistique 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[405].

II) Quant à la publication des jugements, décisions ou accords

11. Les derniers amendements gouvernementaux ont apporté ici une modification au projet de loi initial de sorte que le livre 5 du Code de la consommation précise désormais une publication intégrale du jugement définitif de recevabilité ou d'irrecevabilité ou, le cas échéant la décision définitive en appel[406], l'accord homologué[407], le jugement de responsabilité ou de rejet[408], ainsi que le jugement en cessation et en interdiction[409].

À cet effet, le projet de loi tel que modifié indique[410] que le ministre ayant la Protection des consommateurs dans ses attributions doit publier sans retard sur son site internet tous les jugements en cessation, en interdiction ou en recours collectif ainsi que tout accord extrajudiciaire pour donner aux consommateurs et aux professionnels la possibilité d'agir ou de se manifester.

12. La CNPD comprend d'après le nouvel article L. 524-8 du Code de la consommation en lien avec l'article L. 524-11 du Code de la consommation, tel que modifié, relatif aux mentions d'information – certes non exhaustives – du jugement en responsabilité que les coordonnées du liquidateur ou celle du représentant du groupe seraient indiquées aux fins de faire valoir la demande d'adhésion ou d'exclusion ou de rejet notamment par un consommateur individuel dont la dénomination individuelle ne figurerait pas dans lesdites mentions. A toutes fins utiles, la Commission nationale tient à rappeler l'importance de garantir la protection des données à caractère personnel de toute personne physique

[403] 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, Mém. A 689.
[404] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Article 37, II).
[405] Voir Délibération n°34/AV20/2023 du 5 mai 2023 de la Commission nationale pour la protection des données, point 10.
[406] Voir nouvel article L. 521-2 (3) du Code de la consommation aux fins de transposition des paragraphes 3 et 4 de l'article 13 de la directive (UE) 2020/1828.
[407] Voir nouvel article L. 522-5 (5) du Code de la consommation.
[408] Voir nouvel article L. 524-3 (5) du Code de la consommation.
[409] Voir nouvel article L. 523-1 (3) du Code de la consommation.
[410] Voir notamment articles L. 521-2, 522-4, 523-1 (4) et 524-3 du Code de la consommation.

identifiée ou identifiable dans toute décision judiciaire accessible publiquement.

Malgré l'absence de cadre légal particulier existant au Luxembourg, la CNPD se réfère à la pratique actuelle d'anonymisation de toutes mentions comme les noms, prénoms, adresse, etc. permettant d'identifier une personne physique que ce soit tant les parties au litige que d'éventuels tiers intervenants par les juridictions supérieures et inférieures dans leur publication notamment sur le portail internet de la Justice.

13. Selon le modèle usité, les dénominations des personnes morales, sont aussi en principe anonymisées bien que le RGPD ne s'applique qu'aux personnes physiques. A ce titre, il est aussi utile de rappeler que les informations liées aux noms des administrateurs ou représentants légaux constituent des données à caractère personnel lorsqu'elles se rapportent à des personnes identifiées ou identifiables. Dans l'optique du projet de loi sous étude, la CNPD comprend que le but de ces publications soit notamment de permettre aux personnes concernées individuelles de se joindre au groupe. Ces dernières devraient donc pouvoir avoir un intérêt à reconnaître les décisions concernant leur cas d'espèce et donc d'identifier le professionnel, le cas échéant le responsable du traitement en cause.

14. Ainsi la CNPD se demande quelles seraient, au final, les mentions précises qui figureraient en accès public, en particulier si des données à caractère personnel sont concernées. Si l'obligation de publication des actes mentionnés au point 11 ci-avant s'avère répondre à une exigence légale, encore faudrait-il veiller à bien octroyer des garanties appropriées pour préserver les éventuelles données personnelles des personnes concernées une fois les finalités de traitement réalisées comme notamment par la détermination et le respect de durée(s) de conservation, de publication limitée(s) sur le(s) site(s) internet concerné(s) ou, dans la mesure du possible, par l'emploi de techniques d'anonymisation.

Outre les actes visés au point 11 ci-avant, la Commission nationale note également que le nouvel article L. 511-5 du Code de la consommation prévoit aussi certaines informations publiques à mettre à disposition par le demandeur sur leur site internet et plus particulièrement *« les recours collectifs qu'il a décidé d'intenter, leur état d'avancement et les résultats obtenus ».*

III) Quant à l'articulation des différentes actions et mécanismes existants

15. Dans son avis initial, la CNPD avait déjà évoqué plusieurs interrogations quant aux interactions entre les différents acteurs impliqués, en particulier entre le tribunal d'arrondissement siégeant en matière commerciale et la CNPD. Elle avait aussi soulevé l'importance de veiller à la cohérence globale de l'application uniforme de la législation en matière de protection des données[411].

[411] Voir Délibération n° 34/AV20/2023 du 5 mai 2023 de la Commission nationale pour la protection des données, points 14 et s.

ANNEXES

16. Les derniers amendements gouvernementaux ont apporté certaines modifications premièrement sur le système dit d'opt-in et d'opt-out de sorte qu'une fois les délais tels que définis dans le jugement de responsabilité par le juge pour l'adhésion ou l'exclusion passés, le consommateur qui aurait manifesté sa volonté explicite ou implicite de rejoindre le groupe ne pourrait plus *« entamer une action future quelconque ayant le même objet et la même cause contre le même professionnel »*[412].

Tel qu'exposé dans les commentaires de l'article L.524-4 du Code de la consommation, cette modification est justifiée par la transposition de l'article 9 paragraphe 4 de la directive (UE) 2020/1828 afin notamment d'éviter que les consommateurs ne soient indemnisés plus d'une fois pour une action avec les mêmes objet, cause et partie adverse.

17. La Commission nationale constate que le terme « action » n'est nullement défini comme terme isolé dans le projet de loi ou les amendements gouvernementaux. Néanmoins le nouvel article L.524-4 (3) du Code de la consommation précise le fait que le ou les consommateurs ayant manifesté leur volonté d'être représenté(s) dans le cadre d'un recours collectif se verront exclure *« tout autre recours collectif, accord de médiation ou action à titre individuel ayant le même objet et la même cause contre le même professionnel »*. Ainsi la CNPD se demande quelles sont les actions précisément sous-entendues par cette exclusion ? S'agit-il uniquement d'actions en justice que tout consommateur pourrait intenter à titre individuel en tant que partie demanderesse ? Les réclamations auprès de la CNPD qui pourraient être introduites par un consommateur individuel sont-elles ainsi ou non comprises par les auteurs des amendements dans cette exclusion ?

18. Aussi si les auteurs des amendements gouvernementaux n'entendaient pas exclure le cas d'actions hors voie judiciaire, la Commission nationale estime que la procédure telle que désormais décrite pourrait toujours s'avérer problématique au regard du risque de l'existence d'une procédure parallèle similaire via l'introduction d'une réclamation auprès de la CNPD ou de la décision d'ouverture d'une d'enquête par la CNPD. Les mêmes questions d'ordre procédural tels qu'exposées dans l'avis initial de la CNPD risqueraient alors encore de se poser[413]. En particulier comment le tribunal compétent et la CNPD obtiendraient-ils connaissance mutuellement des recours respectifs ? La CNPD devrait-elle alors systématiquement consulter les sites internet des demandeurs potentiels pour prendre connaissance des recours collectifs intentés[414] ?

Hormis les incertitudes d'ordre procédural, la CNPD s'inquiète toujours plus particulièrement des risques de contradictions potentielles quant à l'interprétation d'une violation des dispositions du RGPD entre les différents recours possibles en lien avec la protection

[412] Voir articles L. 524-12 et L. 524-13 du Code de la consommation, tels que modifiés.
[413] Voir Délibération n°34/AV20/2023 du 5 mai 2023 de la Commission nationale pour la protection des données, points 15, 16 et 17.
[414] Voir le nouvel article L. 511-5 du Code de la consommation et point 11 (2) du présent avis complémentaire.

des données devant les différents acteurs impliqués. Un consommateur qui ne serait pas ou plus partie d'un groupe ne pourrait certes pas prétendre à une indemnisation individuelle via une réclamation intentée auprès de la CNPD. Pour autant la violation des dispositions du RGPD par le même professionnel pourrait être constatée et jugée en parallèle. La CNPD estime donc qu'il serait utile, le cas échéant, que les procédures nationales prévoient avec plus de précisions les modalités d'articulation entre les différentes actions en matière de protection des données au sein d'un même État membre incluant, au besoin, des mécanismes de mise en suspens ou de dessaisissement[415] et se permet de renvoyer pour le surplus aux questions et développements déjà évoqués dans son avis initial.

Sur ce point, la Commission nationale aimerait rappeler à son soutien la conclusion de l'arrêt de la Cour de justice de l'Union européenne du 12 janvier 2023 (C-132/21)[416]. Si la Cour valide bien la possibilité d'introduire de manière concomitante des recours contentieux devant des juridictions administratives et judiciaires prévus par le RGPD, elle précise aussi qu'en l'absence de réglementation de l'Union en la matière et eu égard au risque de décisions contradictoires, il appartient à chaque État membre, en vertu du principe d'autonomie procédurale, de prévoir *« les modalités d'articulation de ces voies de recours afin que soient assurés l'effectivité de la protection des droits garantis par ce règlement [2016/679], l'application cohérente et homogène des dispositions de ce dernier ainsi que le droit à un recours effectif devant un tribunal, visé à l'article 47 de la Charte des droits fondamentaux de l'Union européenne »*[417].

19. La Commission nationale souhaite revenir, deuxièmement, sur une autre modification apportée par les derniers amendements concernant l'ajout des termes *« national(es) ou transfrontière(s) »* après les termes *« en cessation ou en interdiction »* et « recours collectif » à l'article L. 321-4 du Code de la consommation, tel que modifié, et plus spécifiquement sur l'aspect transfrontalier. Il est donc désormais précisé que les entités régulatrices sectorielles instituées, comme la CNPD, peuvent intenter une action en cessation ou en interdiction, ou un recours collectif, national ou transfrontière, autrement dit la possibilité, selon la définition précisée à l'article L. 511-1 du Code de la consommation, tel que modifié, d'intenter un recours dans un État membre autre que celui où l'entité a été désignée.

20. La CNPD se demande ainsi si cet ajout ne risquerait pas quelque peu de venir perturber le mécanisme de coopération et de cohérence tel que prévu par le Chapitre VII du RGPD. Ce dernier implique en effet la désignation d'un interlocuteur unique, en d'autres termes l'autorité chef de file qui est l'autorité de protection des données du pays où se trouve l'établissement principal de l'entreprise ou du professionnel concerné.

[415] Dans le même sens, voir conclusions de l'Avocat Général Jean Richard de la Tour présentées, le 8 septembre 2022, affaire C-132/21, point 49.
[416] Arrêt du 12 janvier 2023, BE c/ Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2.
[417] Ibid., point 57.

ANNEXES

Cette autorité chef de file est ensuite chargée de coordonner la prise de décisions avec les autorités de protection des données concernées par le traitement transfrontalier. L'intervention du CEPD est également prévue en cas de désaccord. De ce fait, si désormais n'importe quelle autorité nationale de protection des données déciderait d'elle-même d'introduire un recours dans un autre État membre que celui lié au professionnel en cause alors que l'autorité chef de file - pouvant être distincte de l'entité régulatrice à l'origine de l'action - devrait en principe coordonner la plainte, n'y aurait-il pas là un nouveau risque de frictions entre lesdites réglementations et procédures en cause ?

21. Finalement, la CNPD se questionne sur les possibles répercussions en cas d'urgence pour la protection des données des droits et libertés des personnes concernées. Le RGPD prévoit ainsi dans son article 66 une dérogation au mécanisme de contrôle de la cohérence et de coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées permettant à une autorité de contrôle concernée d'adopter immédiatement des mesures provisoires dans l'attente éventuelle d'une décision contraignante d'urgence au comité. Ladite procédure d'urgence n'est pas retranscrite au sein de la législation nationale luxembourgeoise dédiée à la protection des données contrairement à d'autres pays voisins[418] dont l'interruption temporaire du traitement litigieux figure parmi l'une des mesures possibles. Le juge administratif, juge des décisions de la CNPD et/ou le juge judiciaire devrait-il être saisi en pareil cas et comment les décisions s'articuleraient-elles de nouveau entre elles ?

22. En conclusion, la CNPD insiste sur l'importance de veiller à la cohérence globale du système et des procédures nationales dans leur ensemble afin de garantir la sécurité juridique de la protection juridictionnelle obtenue.

Ainsi adopté à Belvaux
en date du 16 août 2024.

Pour la Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[418] Voir notamment article 21 de la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

6

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

Délibération n°55/AV23/2024
du 23 août 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Le 26 avril 2024, la CNPD a avisé le projet de règlement grand-ducal relatif à la plateforme de données énergétiques (ci-après le « projet de règlement grand-ducal »)[419].

3. Des amendements gouvernementaux relatifs au projet de règlement grand-ducal ont été transmis le 25 juillet 2024 pour avis à la Commission nationale (ci-après les « amendements »).

4. Tout d'abord, il y a lieu de féliciter les auteurs du projet de règlement grand-ducal pour avoir tenu compte, à l'amendement 3, des remarques émises par la CNPD sous le point 15 de son avis précité et d'avoir modifié en ce sens le texte sous avis.

5. Par ailleurs, il ressort de l'amendement 4 que les auteurs du projet de règlement grand-ducal entendent changer de procédé en ce qui concerne le chiffrement des données traitées sur la plateforme de données énergétiques. En effet, il ressort du commentaire de l'amendement 4 qu'il est désormais prévu de *« mandater le cryptage des disques sur lesquels les données de consommation sont stockées, sans néanmoins demander le cryptage de chaque donnée individuelle sur ces disques »*. Sous réserve que le chiffrement de données reste conforme à l'état de l'art, la Commission nationale prend acte d'un tel changement de méthode. Toutefois, elle estime que des mesures adaptées de

[419] V. Délibération n°21/AV9/2024 du 26 avril 2024 de la Commission nationale pour la protection des données.

ANNEXES

sécurité devront être prises pour compenser les types de risques liés à ce niveau de chiffrement dont le niveau de sécurité est réduit par rapport à un chiffrement au niveau des données.

A toutes fins utiles, la CNPD recommande d'utiliser le terme « chiffrement » alors que l'autorité de contrôle française (la « CNIL ») estime également que l'utilisation du terme de « cryptage » est « impropre ».

6. Enfin, en ce qui concerne les développements soulevés par la Commission nationale dans son avis précité du 26 avril 2024 qui n'auraient pas été suivis par les auteurs du texte en projet, elle se permet de s'y référer et réitère l'ensemble desdits développements.

Ainsi adopté à Belvaux
en date du 23 août 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Alain Herrmann
Commissaire

6

Avis complémentaire de la Commission nationale pour la protection des données relatif au 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'État

Délibération n°56/AV24/2024
du 30 août 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Le 5 juin 2019, la CNPD a avisé le 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'État (ci-après le « projet de loi »)[420].

3. Le 11 juin 2024, la Commission de la Justice a adopté une série d'amendements relative au projet de loi (ci-après les « amendements »).

4. La Commission nationale constate avec satisfaction que les auteurs des amendements ont pris en compte certaines des remarques émises dans son avis initial. Néanmoins, comme d'autres points commentés dans l'avis initial n'ont pas été suivis, et que certaines modifications envisagées apportent des éléments nouveaux, elle s'autosaisit afin de faire part de ses observations ci-après.

I. Remarques liminaires

5. À titre de remarques liminaires, la CNPD souhaite souligner l'importance de la lecture combinée du présent projet de loi avec le projet de loi n°8148 relative à la rétention des données à caractère personnel et portant

[420] V. Délibération n°40/2019 du 5 juin 2019 de la Commission nationale pour la protection des données, doc. parl. N°7424/01.

ANNEXES

modification : 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

En effet, le projet de loi n°8148 consacre les mesures législatives encadrant la conservation des données de trafic et de localisation par les opérateurs de télécommunications et fournisseurs de services de communications électroniques, ainsi que les mesures pouvant être ordonnées afin d'accéder aux données ainsi conservées. Le projet sous avis entend quant à lui créer une plateforme de transmission de données des opérateurs de télécommunications et fournisseurs de services de communications électroniques vers les autorités judiciaires ou le Service de renseignement de l'État (ci-après le « SRE ») et en précise les modalités d'utilisation.

Dès lors, les dispositions desdits projets de loi sont à lire ensemble. En effet, une fois que l'accès à de telles données sera ordonné, sur base des mesures prévues par le projet de loi n°8148, les données seront ensuite transmises à l'aide de la plateforme électronique sécurisée prévue par le projet de loi sous avis. Ainsi, la plateforme sert de moyen pour donner l'accès proprement dit.

6. Dans la mesure où la plateforme électronique sécurisée est étroitement liée aux mesures autorisant l'accès aux données de trafic et de localisation conservées, la CNPD estime que la jurisprudence de la CJUE en matière de rétention des données[421] devrait être prise en compte.

Par exemple, la CJUE exige que les mesures législatives en matière de conservation et d'accès prévoient des garanties suffisantes contre les abus, accès illicite et l'utilisation illicites de ces données[422]. Ne faudrait-il dès lors pas prévoir des garanties à l'égard de la plateforme, notamment en ce qui concerne l'effacement des résultats ainsi que les règles de sécurité tel que l'avait soulevée la CNPD dans son avis initial[423] ?

7. En outre, elle se permet de réitérer également sa préoccupation soulevée dans son avis initial[424], à savoir que la non communication de l'ordonnance elle-même

[421] Arrêt du 8 avril 2014, Digital Rights Ireland e. a., C-293/12 et C-594/12, EU:C:2014:238 ;
arrêt du 21 décembre 2016, Tele2 Sverige et Watson e. a., C-203/15et C-698/15, EU:C:2016:970 ;
arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788 ;
arrêt du 6 octobre 2020, La Quadrature du Net e. a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791 ,
arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790 ;
arrêt du 2 mars 2021 , Prokuratuur, C-746/18, EU:C:2021:152 ;
arrêt du 5 avril 2022, Commissioner of An Garda Siochâna e. a., C-140/20, EU:C:2022:258 ;
arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702 ,
arrêt du 17 novembre 2022, Spetsializiranaprokuratura C-350/21, EU:C:2022:896 ;
arrêt du 30 avril 2024, Procura délia Repubblica pressa il Tribunale di Bolzano, C-178/22, EU:C:2024:371 ; et
arrêt du 30 avril 2024, La Quadrature du Net e. a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370.

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

[423] Délibération n°40/2019 du 5 juin 2019 de la Commission nationale pour la protection des données, doc. parl 7427/01, points III.D et E.

[424] Délibération n°40/2019 du 5 juin 2019 de la Commission nationale pour la protection des données, doc. parl 7427/01, point III.B.

aux opérateurs de télécommunications et fournisseurs de services de communications électroniques risque de porter atteinte au droit de ces derniers de former un recours contre les décisions ordonnant les mesures de conservations et d'accès.

II. Ad Amendement 1

8. La CNPD se félicite du choix des auteurs des amendements d'omettre la notion d'*« opérateur »* en faveur de la notion *« opérateurs de télécommunications et fournisseurs de services de communications électroniques »* prévue dans la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques. Tel que soulevé dans son avis initial, l'utilisation d'une terminologie uniformisée dans les dispositions traitant d'un même sujet est cruciale pour assurer la cohérence et la compréhension des textes.

III. Ad Amendement 2

9. La Commission nationale se félicite des modifications apportées par l'amendement 2, en particulier en ce qui concerne l'adaptation des finalités de la plateforme électronique sécurisée ainsi que la prolongation à 5 ans du délai de conservation des fichiers de journalisation des accès.

10. Elle prend par ailleurs note de la décision, sur base du premier avis du Conseil d'État[425], de supprimer la désignation du Centre des technologies de l'information de l'État (ci-après le « CTIE ») en tant que sous-traitant. À cet égard, il importe de soulever que la répartition des rôles à l'égard des différents devoirs et obligations découlant du RGPD ou de toute autre disposition en matière de protection des données est essentielle. Il est ainsi indispensable que les acteurs impliqués connaissent leurs rôles, devoirs et obligations respectifs, nonobstant le fait que leur détermination découle ou non d'un texte légal.

La Commission nationale comprend du fonctionnement de la plateforme et des traitements y relatifs, que le CTIE agit en tant que sous-traitant pour les autres acteurs impliqués. Ce rôle découle par ailleurs directement de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État. Les autres acteurs impliqués, à savoir le SRE, les autorités judiciaires ainsi que les opérateurs de télécommunications et fournisseurs de services de communications électroniques, seront, toujours d'après la compréhension de la CNPD, à considérer comme responsables du traitement. En effet, chacun de ces acteurs effectue des traitements avec des finalités propres en relation avec la plateforme électrique sécurisée. Dès lors, ils sont à qualifier de responsables du traitement pour leurs traitements de données respectifs.

IV. Ad Amendement 3

11. L'amendement 3 entend premièrement introduire une mesure de repérage à l'article 43-1 du Code de procédure pénale et deuxièmement rendre le recours à

[425] Avis du Conseil d'État du 10 décembre 2019, doc. parl. 7424/3, p. 3.

ANNEXES

la plateforme électronique sécurisée obligatoire. Vu les interrogations soulevées par la CNPD dans son avis initial[426], elle note avec satisfaction ce dernier changement. Il importe néanmoins de soulever quelques observations sur l'introduction de la mesure de repérage à l'article 43-1 du Code de procédure pénale.

12. La Commission nationale ne peut que soutenir les observations du Conseil d'État[427] par rapport à ce troisième amendement. De plus, elle constate que l'amendement ne concerne pas la mise en place de ou la transmission d'informations par la plateforme électronique sécurisée, mais plutôt l'introduction d'une nouvelle mesure de conservation de ou d'accès aux données de trafic et de localisation. Ainsi, il est indispensable que la disposition sous examen respecte la jurisprudence de la CJUE en matière de rétention des données[428], notamment en ce qui concerne les exigences de la Cour vis-à-vis d'une telle disposition législative. La CNPD se demande par ailleurs s'il n'aurait pas été plus cohérent d'inclure une telle disposition dans le projet de loi n°8148 qui traite exclusivement de ces mesures de conservation et d'accès.

13. Étant donné que son avis sur le projet de loi n°8148 détaille les exigences de la CJUE en matière de conservation et d'accès aux données de trafic et de localisation, la CNPD se limite, dans le cadre du présent projet de loi, à soulever plusieurs interrogations, et renvoie, en ce qui concerne les exigences de la CJUE, à son avis précité[429].

14. A la lecture des changements apportés à l'article 43-1 du Code de procédure pénale, il n'est pas clair si l'article consacre une mesure de conservation de données ou une mesure d'accès aux données.

15. Il convient de rappeler que le projet de loi n°8148 introduit un changement de paradigme en ce qui concerne la conservation des données de trafic et de localisation. Le régime actuel consacre le principe d'une conservation généralisée et indifférenciée des données de trafic et de localisation pour 6 mois. En prenant en compte les arrêts de la CJUE, le projet de loi n°8148 interdit cette conservation généralisée et indifférenciée dans tous les cas et la remplace par plusieurs mesures plus restrictives tant en ce qui concerne la

[426] V. Délibération n°40/2019 du 5 juin 2019 de la Commission nationale pour la protection des données, doc. parl. N°7424/01, point IV.
[427] Avis du Conseil d'État du 10 décembre 2019, doc. parl. 7424/3, p. 3.
[428] Arrêt du 8 avril 2014, Digital Rights Ireland e. a., C-293/12 et C-594/12, EU:C:2014:238 ;
arrêt du 21 décembre 2016, Tele2 Sverige et Watson e. a., C-203/15et C-698/15, EU:C:2016:970 ;
arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788 ;
arrêt du 6 octobre 2020, La Quadrature du Net e. a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791 ,
arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790 ;
arrêt du 2 mars 2021 , Prokuratuur, C-746/18, EU:C:2021:152 ;
arrêt du 5 avril 2022, Commissioner of An Garda Siochâna e. a., C-140/20, EU:C:2022:258 ;
arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702 ,
arrêt du 17 novembre 2022, Spetsializiranaprokuratura C-350/21, EU:C:2022:896 ;
arrêt du 30 avril 2024, Procura délia Repubblica pressa il Tribunale di Bolzano, C-178/22, EU:C:2024:371 ; et
arrêt du 30 avril 2024, La Quadrature du Net e. a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370.
[429] Délibération n°28/AV12/2024 de la Commission nationale de la protection des données du 16 mai 2024, doc. parl, n°8148/06.

conservation des données que l'accès aux données ainsi conservées.

Dès lors, il sera désormais nécessaire de décider pour des motifs précis et par une mesure spécifique la conservation des données de trafic et de localisation. Une telle mesure pourra être, par exemple, la conservation ciblée future des données ou encore la conservation rapide (quick freeze) de données dont les opérateurs de télécommunications et fournisseurs de services de communications électroniques disposent encore afin de prévenir leur effacement. La conservation généralisée et indifférenciée ne sera possible que dans des situations de sauvegarde de la sécurité nationale[430].

16. Ainsi, si les amendements visent à une mesure d'accès aux données conservées suivant le régime actuel, il y a lieu de soulever que ce régime a vocation à disparaître avec le projet de loi n°8148. Une fois ce régime changé, la disposition sera vidée de son sens car il n'existera à priori plus de données auxquelles il pourra y être accédé. Dès lors, ne faudrait-il pas introduire une mesure de conservation ciblée ou rapide, voire renvoyer expressément à la mesure de conservation déjà prévue par le projet de loi n°8148 sur base de laquelle les données à accéder ont été conservées ? En tout état de cause, pareille mesure devra répondre aux exigences de la CJUE.

17. En revanche, si les amendements visent à introduire une mesure de conservation des données de trafic et de localisation, il y a lieu de se demander sur base de quelle mesure les données seront par la suite accédées par les autorités.

18. En tout état de cause, il convient de constater que les exigences de la CJUE à l'égard des mesures de conservation ciblée ou rapide ne sont pas respectées. La disposition dans sa rédaction actuelle semble dès lors non conforme à la jurisprudence de la CJUE.

Ainsi adopté à Belvaux
en date du 30 août 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Alain Herrmann
Commissaire

[430] La CJUE admet encore la conservation généralisée et indifférenciée des données d'identification et des adresses IP. De plus amples informations sur toutes les exceptions du principe de non conservation ainsi que des exigences de la CJUE peuvent être trouvées dans l'avis de la CNPD sur le projet de loi n°8148.

ANNEXES

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal portant modification du règlement grand-ducal du 22 janvier 2009 concernant la coopération interadministrative de l'Administration des Contributions Directes et de l'Administration de l'enregistrement et des Domaines

Délibération n°57/AV25/2024
du 30 août 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Par courrier du 22 août 2024, Monsieur le Ministre des Finances a invité la Commission nationale à aviser le projet de règlement grand-ducal portant modification du règlement grand-ducal du 22 janvier 2009 concernant la coopération interadministrative de l'Administration des Contributions Directes et de l'Administration de l'enregistrement et des Domaines (ci-après le « projet de règlement grand-ducal »).

3. Le projet de règlement grand-ducal comporte un article unique qui a pour objet d'introduire un chapitre IIIbis intitulé « Échange automatique ». Il ressort de l'exposé des motifs que les dispositions de l'article 1er du projet de règlement grand-ducal ont pour objet de *« permettre la transmission automatique des données relatives aux extraits de mutations immobilières de l'Administration de l'enregistrement, des domaines et de la TVA à l'Administration des contributions directes, pour les besoins de l'impôt foncier et pour l'établissement des revenus ou bénéfices imposables résultant de mutations immobilières ».* Les auteurs du projet de règlement grand-ducal précisent encore dans le commentaire des articles que « cet échange existe sous format papier depuis 1948 ».

4. Sans préjuger du bienfondé d'un tel échange, la Commission nationale se demande si de telles dispositions ne devraient pas figurer dans la loi du 19 décembre 2008 ayant pour objet la coopération interadministrative et

judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines et de l'Administration des douanes et accises et portant modification d'autres lois, alors que le Conseil d'État a relevé dans son avis relatif au projet de loi portant organisation de l'Administration du cadastre et de la topographie que : *« l'article 31 de la Constitution, qui figure dans la section consacrée aux libertés publiques, dispose que : « [t]oute 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 », tandis que l'article 37 de la Constitution précise, dans sa première phrase, que « [t]oute limitation à l'exercice des libertés publiques doit être prévue par la loi et respecter leur contenu essentiel ».*

« Il s'ajoute à ce rappel des textes fondamentaux que la Cour constitutionnelle, en affinant sa jurisprudence antérieure, a, dans son arrêt n°177 du 3 mars 2023, retenu que « [d]'après l'article 32, paragraphe 32, de la Constitution, dans les matières réservées par la Constitution à la loi, la fixation des objectifs des mesures d'exécution doit être clairement énoncée, de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi ».

« Il y a lieu de déterminer, dans l'ordre juridique national, les conditions dans lesquelles les données à caractère personnel peuvent être traitées pour une finalité autre que celle pour laquelle elles ont été collectées au sens de l'article 6, paragraphe 4, 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, ce qui couvre les hypothèses dans lesquelles des données sont communiquées par une administration à des tiers. Cette communication de données à caractère personnel à des tiers doit être strictement encadrée, ceci en application du droit à la sécurité et la confidentialité découlant du règlement européen précité.

« Afin d'assurer la conformité de la disposition sous examen aux articles 31 et 37 de la Constitution, il convient, sous peine d'opposition formelle, de compléter cette disposition en précisant notamment la nature des données à caractère personnel communiquées à des tiers, la qualité du « tiers intéressé dûment identifié », ainsi que la finalité et les conditions dans lesquelles cet échange a lieu »[431].

En outre, au vu de ce qui précède, et pour plus de cohérence, ne faudrait-il pas également intégrer dans la loi du 19 décembre 2008 précitée l'ensemble des articles du règlement grand-ducal modifié du 22 janvier 2009 concernant la coopération interadministrative de

[431] V. Avis n°61.798 du 12 juillet 2024 du Conseil d'État, doc. parl. n°8330B/2.

ANNEXES

l'Administration des contributions directes et de l'Administration de l'enregistrement, des domaines et de la TVA.

En effet, les articles dudit règlement grand-ducal ont pour objet la gestion d'une base de données commune, prévoient également le principe d'échanges de données entre l'Administration des contributions directes (ci-après l' « ACD ») et l'Administration de l'enregistrement, des domaines et de la TVA (ci-après l' « AED ») ainsi que le principe de contrôles simultanés et communs pouvant être effectués par l'ACD et l'AED concernant des contribuables ou assujettis.

5. En tout état de cause, un tel échange automatique de données devra notamment respecter :
- le principe de minimisation des données visé à l'article 5.1.c) du RGPD ; et
- le principe d'intégrité et de confidentialité visé à l'article 5.1.f) du RGPD

6. Ainsi, en vertu du principe de minimisation des données *« [l]es données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».*

Dès lors, seules les données qui sont adéquates, pertinentes et nécessaires aux fins de la détermination de l'impôt foncier et pour l'établissement des revenus ou bénéfices imposables résultant de mutations immobilières, devraient faire l'objet de l'échange automatique visé par le texte sous avis.

7. Par ailleurs, conformément à l'article 5.1.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 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.

Il y a lieu de rappeler qu'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 l'entité concernée, 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.

La Commission nationale souligne aussi l'importance d'effectuer proactivement des contrôles en interne. À cet effet, il convient conformément à l'article 32.1.d) du RGPD de mettre en œuvre une procédure *« visant à tester, à analyser et à évaluer régulièrement*

6

l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ».

De telles mesures devront, dès lors, être mises en œuvre dans le cadre de l'échange automatique de données, entre l'AED et l'ACD.

Ainsi adopté à Belvaux
en date du 30 août 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Alain Herrmann
Commissaire

ANNEXES

Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif au 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'État

Délibération n°60/AV26/2024
du 31 octobre 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Le 5 juin 2019, la CNPD a avisé le 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'État (ci-après le « projet de loi »)[432]. Suite à des amendements parlementaires adoptées le 11 juin 2024, la CNPD a adopté son avis complémentaire le 30 août 2024[433].

3. Le 15 octobre 2024, la Commission de la Justice a adopté un amendement unique (ci-après l' « amendement ») visant à répondre aux critiques soulevés par le Conseil d'État[434].

4. La Commission nationale regrette que l'amendement et son commentaire ne répondent pas aux interrogations soulevées dans son avis complémentaire. Néanmoins, l'amendement lui permet de mieux comprendre l'intention des auteurs du projet de loi, notamment en ce qui concernent les modifications apportées à l'article 43-1 du Code de procédure pénale.

[432] V. Délibération n°40/2019 du 5 juin 2019 de la Commission nationale pour la protection des données, doc. parl. N°7424/01.
[433] V. Délibération n°56/AV24/2024 du 30 août 2024 de la Commission nationale pour la protection des données, doc. parl. N°7424/06.
[434] V. Avis complémentaire n°53.323 du Conseil d'État du 12 juillet 2024, doc. parl. N°7424/5.

5. En effet, la CNPD comprend désormais que la nouvelle rédaction de l'article 43-1 du Code de procédure pénal entend introduire une mesure d'accès aux données de trafic et de localisation, sans prévoir une mesure de conservation. Ainsi, le procureur d'État peut ordonner que les opérateurs et fournisseurs de services de communications électroniques fournissent pour une durée d'un mois les données de trafic et de localisation qu'ils détiennent à ce moment. Il convient de noter que cette mesure est renouvelable.

6. La CNPD souhaite cependant soulever quelques interrogations quant à la nouvelle mesure d'accès aux données de trafic et de localisation.

7. Tout d'abord, il y a lieu de relever que la disposition sous avis introduit une mesure d'accès et non pas une mesure de conservation. Elle se limite donc à permettre aux autorités compétentes d'accéder aux seules données que les opérateurs et fournisseurs de services de communications électroniques détiennent au moment de l'ordonnance, voire les données qui auraient été collectées par ces derniers durant la durée d'application de l'ordonnance du procureur d'État. Une obligation de conservation ultérieure de telles données par les opérateurs et fournisseurs de services de communications électroniques, pour des finalités ultérieures, c'est-à-dire les objectifs de la recherche de personnes disparues, ne peut pas avoir lieu. Ceci est notamment important à prendre en compte en vue du changement de paradigme que le projet de loi 8148[435] entend apporter. En effet, le projet de loi 8148 entend abroger le principe de conservation généralisée et indifférenciée des données de trafic et de localisation.

Ainsi, pour contraindre les opérateurs et fournisseurs de services de communications électroniques à conserver de telles données, au-delà du délai de conservation prévu pour les finalités de facturation ou de recours en relation avec ces factures[436], il faudrait prévoir une mesure de conservation propre. Il résulte effectivement de la jurisprudence de la Cour de Justice de l'Union européenne (ci-après la « CJUE » ou la « Cour ») que le principe de la hiérarchie des objectifs exige que des données de trafic et de localisation conservées pour, par exemple, des objectifs de sauvegarde de la sécurité nationale ne peuvent pas être accédées pour des objectifs de moindre importance.

Dès lors, l'article 43-1 du Code de procédure pénale ne pourra être utilisé que pour accéder à des données actuellement à disposition des opérateurs et fournisseurs de services de communications électroniques ou éventuellement à des données conservées pour des objectifs avec le même degré d'importance.

En revanche, elle ne pourra pas être utilisée pour accéder à des données conservées pour des finalités avec un degré d'importance plus élevé. Pour des développements plus amples sur le principe

[435] Projet de loi n°8148 relative à la rétention des données à caractère personnel et portant modification: 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.
[436] A noter qu'il existe quelques autres exceptions pour conserver les données de trafic et de localisation.

ANNEXES

de la hiérarchie des objectifs, la CNPD renvoie à son avis relatif au projet de loi n°8148 relative à la rétention des données à caractère personnel et portant modification : 1° du Code de procédure pénale ; 2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et 3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État[437].

8. Il convient encore de rappeler que toute mesure d'accès aux données de trafic et de localisation doit répondre aux exigences de la CJUE en matière de rétention des données[438]. Ainsi, la mesure d'accès sous avis doit être lue à la lumière des arrêts pertinentes de la CJUE.

9. La Cour exige notamment que *« il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales »*[439]. Ainsi, la Cour exige deux choses : une demande motivée par les autorités compétentes qui souhaitent accéder aux données et un contrôle préalable indépendant.

10. Si la CJUE ne donne pas davantage de précisions sur la demande d'accès motivée, que les autorités compétentes doivent soumettre à l'entité qui effectue le contrôle, elle s'est néanmoins prononcée sur le caractère indépendant et préalable de ce contrôle.

11. Premièrement, en ce qui concerne le caractère indépendant du contrôle, la Cour explique que *« l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable [...] impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence*

[437] Délibération n°28/AV12/2024 de la Commission nationale de la protection des données du 16 mai 2024, doc. parl, n°8148/06, notamment point 109.

[438] Arrêt du 8 avril 2014, Digital Rights Ireland e. a., C-293/12 et C-594/12, EU:C:2014:238 ;
arrêt du 21 décembre 2016, Tele2 Sverige et Watson e. a., C-203/15et C-698/15, EU:C:2016:970 ;
arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788 ;
arrêt du 6 octobre 2020, La Quadrature du Net e. a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791 ,
arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790 ;
arrêt du 2 mars 2021 , Prokuratuur, C-746/18, EU:C:2021:152 ;
arrêt du 5 avril 2022, Commissioner of An Garda Siochâna e. a., C-140/20, EU:C:2022:258 ;
arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702 ,
arrêt du 17 novembre 2022, Spetsializiranaprokuratura C-350/21, EU:C:2022:896 ;
arrêt du 30 avril 2024, Procura délia Repubblica pressa il Tribunale di Bolzano, C-178/22, EU:C:2024:371 ; et
arrêt du 30 avril 2024, La Quadrature du Net e. a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370.

[439] Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e. a., C-203/15et C-698/15, EU:C:2016:970, point 120.

d'indépendance implique [...] que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale »[440]. Elle ajoute encore que *« [t]el n'est pas le cas d'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique. En effet, le ministère public a pour mission non pas de trancher en toute indépendance un litige, mais de le soumettre, le cas échéant, à la juridiction compétente, en tant que partie au procès exerçant l'action pénale. La circonstance que le ministère public soit, conformément aux règles régissant ses compétences et son statut, tenu de vérifier les éléments à charge et à décharge, de garantir la légalité de la procédure d'instruction et d'agir uniquement en vertu de la loi et de sa conviction ne saurait suffire à lui conférer le statut de tiers par rapport aux intérêts en cause [...] »*[441]. La CJUE finit par conclure que *« le ministère public n'est pas en mesure d'effectuer le contrôle préalable »*[442].

12. Deuxièmement, la Cour souligne encore à plusieurs reprises le caractère préalable du contrôle. En effet, elle n'admet un contrôle postérieur qu'en cas d'urgence dûment justifiés[443]. Elle exige par ailleurs que le contrôle a posteriori intervient *« dans de brefs délais »*[444].

13. Dans la mesure où la disposition sous avis entend laisser l'appréciation de la nécessité de la mesure au seul procureur d'État, la CNPD se demande si les exigences de la CJUE concernant le contrôle indépendant et préalable sont remplies.

14. Ensuite, la CJUE exige que la législation nationale prévoit des garanties effectives contre les risques d'abus. Ainsi, la CJUE demande à ce que les *« autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités »*[445]. En effet, cette information est nécessaire pour permettre aux personnes dont les données ont été accédées d'exercer leurs droits. Il est effectivement impossible pour une personne d'exercer ses droits s'il n'est pas au courant de la situation.

15. Étant donné que l'amendement sous avis n'entend pas introduire une telle information à fournir aux personnes concernées, la CNPD estime que l'exigence de la CJUE n'est pas respectée.

16. Enfin, la CJUE soulève que l'accès ne peut avoir lieu que dans la limite du strict nécessaire. Elle décide *« dès lors qu'un accès général à toutes les données conservées,*

[440] Arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 54.
[441] Ibid. points 55 et 56.
[442] Ibid. point 57.
[443] Voir par exemple arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 120.
[444] Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 110.
[445] Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 121.

ANNEXES

indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire [...] »[446]. La Cour explique que *« la réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des abonnés ou des utilisateurs inscrits. À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction (voir, par analogie, Cour EDH, 4 décembre 2015, Zakharov c. Russie, CE:ECHR:2015:1204JUD004714306, § 260). Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités »*[447].

17. Au vu de ce qui précède, la CNPD se demande encore si la rédaction actuelle de la disposition répond aux critères de la CJUE en ce qui concerne la limitation au strict nécessaire. En effet, la disposition reste muette sur le choix des personnes dont les données pourraient être accédées, ou pour tout le moins elle ne contient pas de conditions ou critères permettant de délimiter ces personnes. Tel que soulevé par la CJUE, il devrait au moins exister un lien indirect entre l'objectif recherché (la recherche de la personne) et les personnes dont les données seront accédées.

Ainsi adopté à Belvaux
en date du 31 octobre 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Alain Herrmann
Commissaire

Marc Lemmer
Commissaire

[446] Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.
[447] *Ibid.*

6

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8421 sur la promotion du journalisme professionnel et du débat démocratique, portant modification : 1° de la loi modifiée du 8 juin 2004 sur la liberté d'expression dans les médias ; 2° de la loi modifiée du 14 septembre 2018 relative à une administration transparente et ouverte ; 3° de la loi du 30 juillet 2021 relative à un régime d'aides en faveur du journalisme professionnel.

Délibération n° 63/AV27/2024
du 7 novembre 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après la « Commission nationale » ou la « CNPD ») *« conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

2. Par ailleurs, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

3. N'ayant pas été directement saisie par le Ministère d'État, la Commission nationale souhaite néanmoins se prononcer quant au projet de loi n°8421 sur la promotion du journalisme professionnel et du débat démocratique, portant modification : 1° de la loi modifiée du 8 juin 2004 sur la liberté d'expression dans les médias ; 2° de la loi modifiée du 14 septembre 2018 relative à une administration transparente et ouverte ; 3° de la loi du 30 juillet 2021 relative à un régime d'aides en faveur du journalisme professionnel (ci-après le « projet de loi »).

4. Il ressort de l'exposé des motifs que le projet de loi poursuit un triple objectif.

Tout d'abord il vise à renforcer le rôle des journalistes dans le débat public en facilitant leur accès aux informations détenues par les institutions publiques. Ainsi, les auteurs du projet de loi proposent de modifier la loi modifiée du 14 septembre 2018 relative à une administration transparente et ouverte (ci-après la « Loi ATO ») en y introduisant un droit d'accès spécifique aux informations pour les journalistes professionnels. D'autres modifications visent encore à rendre le cadre légal national conforme à la Convention du Conseil de l'Europe sur l'accès aux documents publics, faite à Tromsø le 18 juin 2009 (ci-après la « Convention de Tromsø »), permettant ainsi au Luxembourg de signer et de ratifier ladite Convention.

ANNEXES

En outre, le projet de loi adapte la loi du 30 juillet 2021 relative à un régime d'aides en faveur du journalisme professionnel pour y tenir compte du bilan des premières années de son application et afin de soutenir des projets médiatiques diversifiés.

Enfin, le projet de loi prévoit de mettre à jour la définition du journaliste professionnel dans la loi modifiée du 8 juin 2004 sur la liberté d'expression dans les médias, afin de clarifier particulièrement les critères d'octroi de la carte de presse.

5. La Commission nationale formulera dans le présent avis ses observations relatives aux problématiques ayant trait à la protection des données à caractère personnel soulevées par le projet de loi. Elle se limitera donc à commenter les modifications proposées à la Loi ATO. Dans un premier temps, elle clarifiera le champ d'application de la loi (I), puis examinera le droit d'accès spécifique pour les journalistes professionnels instauré par le projet de loi (II) et l'introduction d'une définition du terme « document » (III).

I. Sur le champ d'application de la Loi ATO

6. La Loi ATO prévoit un droit d'accès aux documents qui sont « détenus par les administrations et services de l'État, les communes, les syndicats des 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, dans la mesure où les documents sont relatifs à l'exercice d'une activité administrative ». Les personnes physiques et morales ont également accès aux documents détenus par la Chambre des Députés, le Conseil d'État, la Cour des comptes et les Chambres professionnelles. Les auteurs du projet de loi ont prévu de compléter cette énumération en ajoutant d'autres organismes rattachés à la Chambre des Députés, à savoir l'Ombudsman, l'Ombudsman fir Kanner a Jugendlecher et le Centre pour l'égalité de traitement.

7. Il est également prévu d'ajouter à l'article 1er la notion d'« autorités judiciaires ». Selon le commentaire des articles, cet ajout vise à mettre la loi en conformité avec les exigences de l'article 1er, paragraphe 2, lettre a), point i, point 2° de la Convention de Tromsø, qui prévoit qu'il faut entendre par « autorités publiques », les organes législatifs et les autorités judiciaires dans la mesure où ils accomplissent des fonctions administratives selon le droit national.

II. Sur le droit d'accès spécifique pour les journalistes professionnels

A. Remarques liminaires

8. Dans le cadre des obligations découlant de l'article 10 de la Convention européenne des Droits de l'Homme, il importe de mettre en place un cadre législatif complet qui permet aux journalistes de contribuer au débat public de manière effective. La reconnaissance du rôle particulier des journalistes professionnels qui requièrent un accès aux informations pour remplir leurs missions d'intérêt général est l'un des objectifs du projet de loi. Ainsi, l'article 5.2° du projet de loi introduit une obligation légale pour les organismes visés par la Loi ATO de fournir aux journalistes professionnels les informations relatives à une activité

administrative, nécessaires à l'exercice de leurs fonctions, telles que définies dans la loi sur la liberté d'expression dans les médias. La CNPD prend acte que, selon le commentaire des articles, cet ajout s'inspire des législations des Länder allemands.

B. Sur les besoins spécifiques des journalistes

9. Le projet de loi prévoit dans son article 8.2 que les *« organismes sollicités tiennent compte, dans les limites du raisonnable, des besoins particuliers des journalistes professionnels »*. Le commentaire des articles précise que cette disposition *« s'explique par les contraintes des journalistes de pouvoir effectuer leurs recherches en tenant compte de l'actualité, en vue de pouvoir informer les lecteurs en temps utiles ».* Cependant, cette disposition reste vague quant à son application pratique. Dès lors, il est recommandé aux auteurs du projet de loi que des précisions soient fournies aux administrations sur la manière d'identifier, dans les limites du raisonnable, les besoins spécifiques des journalistes ainsi que sur les modalités concrètes pour y répondre dans le projet de texte.

10. En outre, le texte proposé prévoit qu'un silence prolongé de l'administration soit interprété comme un refus de communication. Cette disposition vise à offrir une sécurité juridique accrue aux demandeurs, en garantissant qu'après l'expiration du délai prévu à l'article 5.1 de la loi ATO, le demandeur soit en présence d'une décision de l'administration qu'il pourra contester devant la Commission d'accès aux documents, voire le tribunal administratif. Cette modification vise à mettre la loi en conformité avec l'article 8, paragraphe 1er de la Convention de Tromsø.

III. <u>Sur la définition de « document » et la possibilité d'occulter des informations</u>

11. La CNPD note avec satisfaction l'introduction d'une définition du terme « document », qui s'inspire de l'article 1er, paragraphe 2, lettre b) de la Convention de Tromsø. Cette définition précise qu'un document représente toutes informations disponibles enregistrées sous quelque forme que ce soit, rédigées ou reçues et détenues par les organismes visés par la loi. Il y a lieu de saluer les auteurs du projet de loi d'avoir clarifié cette notion conformément aux recommandations émises par la CNPD dans un avis antérieur[448].

12. Comme soulevé par le Conseil d'État dans son avis relatif au projet de loi relative à une administration transparente et ouverte, en étudiant les textes étrangers on constate que la définition de ce qu'est un « document administratif » ne dépend pas du support utilisé, mais se réfère le plus souvent à la notion d'information[449]. L'administration ne peut évidemment donner suite à une demande d'accès que si l'information demandée existe et est consignée dans un document identifiable, quel qu'en soit le support. Selon la compréhension de la CNPD, ce cadre doit être interprété comme

[448] Voir Délibération n° 196/2016 du 26 février 2016, p.3.
[449] Voir avis du Conseil d'État du 28 février 2017, doc. parl. 6810/05, p.1.

ANNEXES

limitant ainsi les demandes d'informations aux données déjà en possession de l'administration, sous forme de documents au sens large.

13. Par ailleurs, le projet de loi permet d'occulter les données dans les documents demandés non seulement lorsqu'ils contiennent des données personnelles conformément à l'article 6.1 de la loi ATO, mais également dans le contexte des exceptions prévues à l'article 1.2 de la loi susmentionnée. Selon les auteurs du projet de loi, cette approche, inspirée du droit français[450], vise à mettre la loi en conformité avec l'article 6 paragraphe 2 de la Convention de Tromsø. La CNPD salue cette mesure, qui permet aux organismes de répondre aux demandes d'accès même lorsque certaines informations doivent être protégées.

14. En résumé, le projet de loi prévoit la possibilité de fournir des documents aux demandeurs dont certains passages sont noircis, ce qui permet de communiquer des documents visés par des exceptions à l'obligation de communiquer. Toutefois, l'accès peut être refusé si le document noirci deviendrait trompeur ou vidé de sens, ou si la mise à disposition du document est une charge manifestement déraisonnable pour l'organisme concerné.

Ainsi adopté à Belvaux
en date du 7 novembre 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[450] Art. L.311.7 du Code des relations entre le public et l'administration.

6

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°8317 relative à la transition énergétique et modifiant : 1° la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité ; et 2° la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz nature

Délibération n°68/AV28/2024
du 15 novembre 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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, l'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Par courrier en date du 26 septembre 2023, Monsieur le Ministre de l'Énergie et de l'Aménagement du territoire a invité la Commission nationale à se prononcer au sujet du projet de loi relative à la transition énergétique et modifiant : 1° la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité ; et 2° la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz nature (ci-après le « projet de loi »).

3. Il ressort de l'exposé des motifs que le projet de loi a pour objet de créer un cadre normatif visant à promouvoir l'efficacité énergétique et à accélérer le développement des énergies renouvelables sur le territoire luxembourgeois. En effet, le projet de loi incorpore les objectifs établis par le Plan national intégré en matière d'énergie et de climat (PNEC) et prévoit l'abrogation de la loi modifiée du 5 août 1993 concernant l'utilisation rationnelle de l'énergie (ci-après la « Loi de 1993 »).

4. La Commission nationale formulera dans le présent avis ses observations relatives aux problématiques ayant trait à la protection des données à caractère personnel soulevées par le projet de loi. Il est important de noter que certaines dispositions du projet de loi traitent des aspects liés au respect de la vie privée et à la protection des données à caractère personnel (I). Il s'agit notamment des dispositions relatives au registre des certificats de performance énergétique authentifiés (II) et celles relatives au registre de la chaleur (III).

ANNEXES

I. Remarques générales

5. En premier lieu, il faut souligner que le RGPD s'applique dès lors qu'un traitement de données personnelles a lieu. L'article 4 du RGPD définit comme données à caractère personnel *« 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 ».* En conséquence, les données traitées en vertu du projet de loi constituent des données à caractère personnel dès lors qu'elles puissent être reliées à une personne physique identifiée ou identifiable.

6. Il y a lieu de rappeler que le RGPD définit le traitement de données 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 ».* Ainsi, toute initiative de collecte et d'échange de données dans le cadre du projet de loi devra intégrer des mesures rigoureuses de protection des données afin de respecter les exigences du RGPD.

7. La CNPD constate que le registre des certificats de performance énergétique contient des données détaillées sur la performance énergétique des bâtiments, ainsi que des informations sur les propriétaires et résidents. De plus, le cadastre de chaleur inclut des informations géographiques sur les sources et réseaux de chaleur et de froid, ainsi que sur les besoins énergétiques des bâtiments. Bien que ces données soient principalement techniques, elles peuvent inclure des informations personnelles lorsque les bâtiments peuvent être reliés à des propriétaires ou résidents spécifiques. La CNPD y reviendra plus particulièrement dans les développements ci-après.

II. Le registre des certificats de performance énergétique authentifiés

A. Remarques liminaires

1. Sur la proposition de modification de la directive 2010/31/UE

8. Le projet de loi vise l'instauration d'une base légale pour un registre de données sur la performance énergétique et la performance environnementale des bâtiments. Il ressort du commentaire des articles qu'*« [a]fin de respecter la directive européenne sur la performance énergétique des bâtiments, la mise en place d'une solution informatique permettant le stockage et la consultation des différentes données concernant la performance énergétique des bâtiments est nécessaire ».*

9. En effet, la proposition de modification de la directive européenne 2010/31/UE sur la performance énergétique des bâtiments (COM/2021/558 final) prévoit que la tenue d'un registre est une obligation des États membres de l'Union européenne. Par conséquent, les auteurs du projet de loi anticipent cette modification et proposent l'introduction d'une base légale pour la mise en place d'une solution informatique permettant la collecte, la sauvegarde et le traitement des différentes données concernant la performance énergétique des bâtiments.

2. Sur l'article 27 du projet de loi et l'article 19 du règlement grand-ducal modifié du 9 juin 2021 concernant la performance énergétique des bâtiments

10. Le projet de loi dans sa section I[ère] sur la performance énergétique et environnementale des bâtiments reprend les grands principes, conditions et obligations consacrés par le règlement grand-ducal modifié du 9 juin 2021 concernant la performance énergétique des bâtiments, désigné par les auteurs du projet de loi comme « Règlement CPE ».

11. La CNPD constate que l'article 27 du projet de loi sous avis reprend certaines des dispositions de l'article 19 du règlement CPE qui dispose que *« [l]e ministre peut tenir un registre des calculs de performance énergétique et des certificats de performance énergétique délivrés par les personnes définies à l'article 4, paragraphe 8. Le ministre définit les éléments d'information qui doivent figurer dans ce registre »*. La CNPD salue cette initiative en soulignant que le traitement des données à caractère personnel relève d'une matière réservée à la loi en vertu de l'article 31 de la Constitution. En effet, l'article 31 de la Constitution, qui figure dans la section consacrée aux libertés publiques, dispose que *« [t]oute 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 »*. L'article 37 de la Constitution dispose notamment que *« [t]oute limitation à l'exercice des libertés publiques doit être prévue par la loi et respecter leur contenu essentiel »*. Dès lors, les éléments essentiels de la matière réservée à la loi doivent, conformément aux principes constitutionnels, être fixés dans la loi formelle et seuls les éléments moins essentiels peuvent être relégués au règlement grand-ducal, afin de prévenir tout risque d'inconstitutionnalité au regard de l'article 102 de la Constitution.

3. Sur l'article 6.3 du RGPD

12. 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 quant à la mise en œuvre du registre des certificats de performance énergétique authentifiés conformément à l'article 6.3 du RGPD.

13. L'article 6.3 du RGPD 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. Les finalités du traitement sont définies

ANNEXES

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 ».

14. 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.

15. 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 (...) ».*

16. 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 ».*

17. 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 ainsi que les durées de conservation des données. Or, force est de constater que certains de ces éléments ne figurent pas ou ne sont pas détaillés avec

suffisamment de précision par l'article 27 du projet de loi. La CNPD y reviendra dans ses développements ci-après.

B. Quant au responsable du traitement

18. Il y a lieu de rappeler que la notion de responsable du traitement joue un rôle capital dans l'application du RGPD dans la mesure où elle détermine qui est responsable du respect des différentes règles en matière de protection des données ainsi que la manière dont les personnes concernées peuvent exercer leurs droits[451]. Dès lors, il est important de pouvoir identifier correctement quelle entité est responsable du traitement.

19. L'article 27.1 du projet de loi dispose qu'*« [i]l est établi, dans le respect des exigences de la législation en matière de protection des données et de la vie privée, un registre de données sur la performance énergétique et la performance environnementale des bâtiments tenu par le ministre qui en assure, dans les limites prévues au paragraphe 6, le rôle de responsable de traitement visé par l'article 4, point 7, du [RGPD] ».* Par ailleurs, l'article 27.6 dispose que *« [l]e ministre est responsable de la sauvegarde et de la gestion administrative des données contenues dans le registre ainsi que de l'authentification visée au paragraphe 4, alinéa 1er. Il ne contrôle pas systématiquement le contenu des données importées et ne saurait dès lors en être tenu responsable ».*

20. La CNPD comprend ainsi que le ministre serait le responsable du traitement en ce qui concerne les traitements de données effectués dans le cadre du registre des certificats de performance énergétique authentifiés.

21. Il convient de rappeler qu'en vertu de l'article 5.1 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 (exactitude) ».* En effet, les dispositions du projet de loi sous avis ne devraient pas décharger le responsable du traitement des obligations qui lui incombent en vertu du RGPD. Ainsi, l'article 27.6 du projet de loi ne devraient pas exclure la responsabilité du ministre quant à l'exactitude des données qui seraient importées dans ledit registre. Les autres entités, en tant que responsables de leurs propres activités de traitement, sont chargées de veiller à l'exactitude des données qu'elles ont traitées auparavant et qu'elles communiquent ensuite au ministre[452].

22. Par ailleurs, l'article 27.4 du projet de loi prévoit que les personnes

[451] V. en ce sens: Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, p. 3, disponibles sous : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[452] V. en ce sens: Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, point 72, disponibles sous : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

ANNEXES

habilitées importent, via une plateforme gouvernementale sécurisée les données requises par la présente loi dans le cadre de l'établissement du certificat de performance énergétique. La Commission nationale s'interroge sur l'entité qui serait chargée de la gestion d'une telle plateforme, notamment si celle-ci est également opérée par le ministre ou par une autre entité. Des clarifications à ce sujet mériteraient d'être apportées par les auteurs du projet de loi. En tout état de cause, en ce qui concerne l'accès et la gestion de ladite plateforme gouvernementale, le responsable du traitement devrait mettre en œuvre des mesures de sécurité afin d'assurer la confidentialité et la sécurité des données. Sur ce point, il est renvoyé au titre IV du présent avis.

C. Quant aux catégories de données à caractère personnel

23. L'article 5.1 c) du RGPD dispose que les données à caractère personnel doivent être *« adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ».* Il résulte de ce principe que ne doivent être traitées que les données nécessaires à l'accomplissement de la finalité du traitement.

24. En l'espèce, l'article 27.3 du projet de loi sous avis énumère les catégories de données sur lesquelles le registre porte. La CNPD rappelle l'importance du principe de minimisation des données, selon lequel seules les données nécessaires à la réalisation des finalités définies à l'article 27.2 du projet de loi peuvent être traitées. Il est essentiel de s'assurer que les données collectées et conservées soient strictement limitées à celles qui sont pertinentes et adéquates pour les objectifs du registre, afin de respecter les exigences du RGPD et de protéger les droits des personnes concernées.

25. À cet égard, il y a lieu de regretter que le projet de règlement grand-ducal, n'ait pas été transmis en même temps que le projet de loi pour connaître les données contenues dans le calcul de performance énergétique et le certificat de performance énergétique authentifié.

26. En outre, il convient de se demander si, dans le cadre de la procédure de contrôle visée à l'article 27.4 du projet de loi, des données à caractère personnel seraient collectées et amenées à figurer dans le registre visé à l'article 27.3 du projet de loi.

27. La CNPD regrette l'absence de précision concernant les catégories de données, qui devraient être intégrées dans le registre. Le texte du projet de loi devrait énumérer de manière exhaustive les catégories de données qui pourrait y figurer, tout en veillant à respecter le principe de minimisation des données.

D. Quant aux finalités

28. L'article 27.2 du projet de loi énumère de manière limitative les finalités du traitement des données afférentes au registre des certificats de performance énergétique en disposant que *« [l]e registre visé au paragraphe 1er a pour finalité de :*

1° servir comme répertoire central mettant de manière efficace, conviviale et sécurisée à la disposition des personnes

visées au paragraphe 7, des données auxquelles elles ont légitimement droit d'accéder ;
2° assurer la conservation des données importées à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques ;
3° améliorer l'accessibilité aux informations et données ainsi que leur qualité ;
4° permettre l'élaboration et la mise à disposition de statistiques et de données agrégées et anonymisées à des fins d'information, de transparence et de recherche ».

29. Bien qu'il y ait lieu de saluer l'effort d'énumération des finalités poursuivis par le registre, force est de constater que certaines desdites dispositions ne respectent 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[453].

30. Il convient de rappeler que la notion de « finalité », c'est-à-dire l'objectif poursuivi par le traitement, occupe une place primordiale au sein du RGPD. Aux termes de l'article 5.1.b) du RGPD, les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

31. De plus, les principes de minimisation des données[454] ou de limitation de conservation[455] s'apprécient au regard des finalités pour lesquelles les données sont traitées. Il est donc essentiel que les finalités du registre soient clairement définies dans le projet de loi. À cet égard, la CNPD estime nécessaire que les auteurs du projet de loi clarifient ces finalités en tenant compte des observations formulées ci-après.

1. Sur les finalités énumérées à l'article 27.2.1° et 27.2.3° du projet de loi

32. L'article 27.2.1° dispose que le registre sert *« comme répertoire central mettant de manière efficace, conviviale et sécurisé à la disposition des personnes visées au paragraphe 7, des données auxquelles elles ont légitimement droit d'accéder ».* Il convient de se demander s'il est pertinent de préciser que les personnes visées au paragraphe 7 ont accès audit registre, alors que les dispositions dudit paragraphe prévoient un tel accès. La Commission nationale propose ainsi d'omettre de telles dispositions et suggère la formulation suivante *« le registre visé au paragraphe 1er a pour finalité de servir comme répertoire central de données sur la performance énergétique et la performance environnementale des bâtiments ».*

Par ailleurs, l'article 27.2.3° prévoit une autre finalité notamment l'amélioration de

[453] 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, Vavřička et autres c. République tchèque (requêtes n°47621/13 et 5 autres), § 276 à 293, 8 avril 2021.
[454] Article 5.1 c) du RGPD.
[455] Article 5.1 e) du RGPD.

ANNEXES

« l'accessibilité aux informations et données ainsi que leur qualité ». Si les auteurs du projet de loi ne devaient pas tenir compte de la proposition de la CNPD formulée ci-avant, elle s'interroge sur la différence entre ces deux finalités, qui semblent se recouper. En effet, l'objectif de rendre les données accessibles de manière efficace, conviviale et sécurisée paraît étroitement lié à celui d'améliorer l'accessibilité et la qualité des informations et des données. Afin d'assurer une meilleure lisibilité des dispositions, ne serait-il pas préférable de regrouper ces finalités sous une finalité unique ?

2. Sur les finalités énumérées à l'article 27.2.2° du projet de loi

33. L'article 27.2.2° du projet de loi précise d'ailleurs que le registre a pour finalité *« la conservation des données importées à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques ».* La Commission nationale souligne que le traitement ultérieur à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales à condition d'être soumis, conformément à l'article 89.1 du RGPD, à des garanties appropriées pour les droits et libertés de la personne concernée[456]. La pseudonymisation, voire l'anonymisation, sont mises en avant par l'article 89.1 du RGPD comme des mesures permettant de garantir les droits et libertés des personnes concernées.

34. Il est également rappelé que l'article 65 de la loi précitée du 1er août 2018 portant organisation de la Commission nationale pour la protection des données doit être respecté dans le cadre des traitements de données mis en œuvre à des fins statistiques ou à des fins de recherche scientifique. La CNPD estime indispensable que le responsable du traitement veille au respect des dispositions précitées. Ledit article prévoit une liste de mesures appropriées à mettre en place par le responsable d'un traitement lorsqu'il traite des données personnelles à des fins de recherche scientifique ou à des fins statistiques. Parmi les mesures listées par cette disposition, on peut également retenir l'anonymisation ou la pseudonymisation (3°) ou encore le recours à un tiers de confiance fonctionnellement indépendant du responsable du traitement pour l'anonymisation ou la pseudonymisation des données (4°).

35. Cependant, les dispositions nationales précitées ne s'appliquent pas aux traitements à des fins archivistiques. De tels traitements lorsqu'ils sont effectués dans l'intérêt public sont, en principe, encadrés par la loi du 17 août 2018 relative à l'archivage. Dès lors, il conviendrait de vérifier que les dispositions envisagées s'articulent correctement avec les

[456] Art. 89.1 du RGPD : *« Le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est soumis, conformément au présent règlement, 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. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière. »*

dispositions de la loi du 17 août 2018 relative à l'archivage.

36. Par ailleurs, il y a lieu de noter que l'article L.126-32 du Code de la construction et de l'habitation français dispose que : *« [...] Ces informations [diagnostics de performance énergétique ou les audits énergétiques] sont transmises à des fins d'information, de contrôle, d'études statistiques, d'évaluation, d'amélioration méthodologique, de mise en œuvre et de suivi des politiques publiques touchant à la construction, aux bâtiments, aux logements, aux consommations énergétiques et aux performances environnementales [...] ».*

Dès lors, il est suggéré aux auteurs du projet de loi de s'inspirer du degré de détail des finalités énoncées dans le texte de loi français en ce qui concerne la formulation des finalités des traitements visées à l'article 27.2.2° du projet de loi sous avis. Il est ainsi proposé de formuler lesdites dispositions en ces termes *« la conservation des données importées à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques en lien avec la performance énergétique et la performance environnementale des bâtiments ».*

Enfin, les dispositions françaises précitées prévoient expressément que *« [c]es informations ne peuvent pas être utilisées à des fins commerciales ».* La CNPD recommande d'introduire une telle interdiction dans les dispositions du projet de loi sous avis.

3. Sur les finalités énumérées à l'article 27.2.4° du projet de loi

37. L'article 27.2.4° du projet de loi prévoit que le registre a pour finalité de *« permettre l'élaboration et la mise à disposition de statistiques et de données agrégées et anonymisées à des fins d'information, de transparence et de recherche ».* En outre, il ressort du commentaire des articles que *« le registre de performance énergétique permet également la mise à disposition de données non-agrégées aux personnes y ayant légalement droit ainsi que de données agrégées et de statistiques en « open data » ».*

38. La CNPD comprend que le registre de performance énergétique permet la mise à disposition de données agrégées et de statistiques, ce qui s'aligne avec la stratégie nationale pour la promotion de l'Open data au Luxembourg. En effet, les détenteurs de données publiques devraient concevoir lesdites données dans l'optique de rendre celles-ci réutilisables.[457]

39. 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 alors que l'entité publique n'exerce qu'une influence limitée sur cette réutilisation. À cet effet, la CNPD souhaite souligner l'importance de la lecture combinée du présent projet de loi avec la loi du 29 novembre 2021 sur les données ouvertes et

[457] V. Délibérationn°01/2021 du 20 janvier 2021 de la Commission nationale pour la protection des données, doc. parl. 7643/02, p.6.

ANNEXES

la réutilisation des informations du secteur public. Il est conseillé aux auteurs du projet de loi de s'assurer que les dispositions envisagées par le projet de loi soient compatibles avec celles prévues par la loi du 29 novembre 2021 précitée.

E. Quant à l'accès par le ministre aux registres visés à l'article 27.5 du projet de loi

1. Remarques générales

40. La CNPD comprend que l'accès aux registres mentionnés à l'article 27.5 du projet de loi vise principalement à vérifier les données requises par la loi en projet et à établir des sources authentiques. Cependant, en ce qui concerne l'accès du ministre aux données du RNPP et du RCS, il résulte du commentaire des articles que cet accès est conféré au ministre « pour les besoins de l'agencement du registre ainsi que du traitement et de la mise à disposition des données ». Toutefois, la CNPD estime que ces explications sont imprécises et ne permettent pas de comprendre quelles seraient les raisons exactes pour lesquelles le ministre aurait besoin des accès aux registres précités. Des clarifications à ce sujet devraient être apportées par les auteurs du projet de loi. Sur ce point, il est renvoyé aux développements formulés sous les points 44 à 46 du présent avis.

41. Par ailleurs, il convient de se demander comment cet accès s'articule avec les dispositions de l'article 27.4.2 du projet de loi. En effet, le ministre contrôle l'exhaustivité des données concernées et procède à l'authentification des certificats de performance énergétique. De plus, il peut préalablement procéder à un contrôle sommaire de l'exactitude des données concernées. Dans le cadre dudit contrôle, le ministre peut exiger la production de tout document nécessaire à la vérification de l'exactitude du certificat concerné. Ainsi, la CNPD comprend que le contrôle opéré par le ministre ne s'effectue pas de manière systématique et qu'il est rendu possible grâce à un accès aux registres. À cet égard, il serait pertinent de clarifier dans quelle mesure cet accès est limité aux contrôles sommaires, ou le cas échéant s'il est conçu pour s'étendre au-delà des seuls contrôles prévus par l'article 27.4.2 du projet de loi.

2. Sur l'accès aux registres du cadastre

42. Il y a lieu d'attirer l'attention des auteurs du projet de loi sur le fait qu'un projet de règlement grand-ducal concernant notamment la consultation et la diffusion de la documentation relative à la mensuration officielle, de la documentation cadastrale, de la documentation topographique, du registre national des localités et des rues et des systèmes de référence de coordonnées nationaux gérés par l'Administration du cadastre et de la topographie a été déposé et a vocation à abroger et remplacer 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 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.

Les articles 5 et 6 dudit projet de règlement grand-ducal entendent encadrer :

- la consultation et délivrance des extraits de la documentation relative à la tenue à jour du registre foncier et de la documentation relative à la tenue à jour du plan cadastral ; et
- l'accès en ligne d'une partie ou l'intégralité du registre foncier.

43. Ainsi, il convient de se demander à quels registres de l'administration du cadastre et de la topographie, le ministre pourrait avoir accès. Afin de s'assurer que les dispositions du projet de loi sous avis et celles du projet de règlement grand-ducal précité, s'articulent correctement, les auteurs du projet de loi devraient préciser expressément les registres auxquels le ministre pourrait avoir accès.

3. Sur l'accès au RNPP et au RCS

44. Le projet de loi accorde au ministre le pouvoir de consulter le registre national des personnes physiques (ci-après le « RNPP ») ainsi que le registre de commerce et de sociétés (ci-après le « RCS »). Ainsi, il résulte de l'article 27.5 du projet de loi que le ministre peut accéder aux données des registres précités afin de vérifier certaines données prévues par le projet de loi et d'établir des sources authentiques pour identifier les propriétaires et les résidents des bâtiments concernés, ainsi que les personnes habilitées.

45. Il convient de regretter que les auteurs du projet de loi ne détaillent pas davantage les raisons pour lesquelles il serait nécessaire de consulter de telles données pour les finalités énumérées par les dispositions du projet de loi sous avis. La CNPD s'interroge plus particulièrement sur la nécessité de vérifier l'identification des résidents des bâtiments faisant l'objet des certificats de performance énergétique.

46. En outre, l'accès au RNPP 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. Dès lors, la CNPD estime que cette disposition du projet de loi pourrait être omise sinon reformulée afin d'être alignée sur le cadre légal en vigueur.

F. Quant à l'accès au registre des certificats de performance énergétique authentifiés

47. La Commission nationale constate que l'article 27.7 du projet de loi prévoit un accès au registre des certificats de performance énergétique authentifiés pour certaines catégories de personnes, notamment les ***« personnes habilitées »,*** **ainsi que les propriétaires et résidents** des bâtiments concernés.

48. Plus précisément, il résulte de l'article 27.7.1° que les personnes habilitées à établir le calcul de performance énergétique et le certificat de performance énergétique peuvent importer, consulter et exporter les données et les documents du registre. À la lecture de ladite disposition, il n'est pas clair s'il s'agit seulement des données et documents que les personnes habilitées ont

ANNEXES

établies elles-mêmes ou toutes les données et documents figurant dans le registre.

49. Il conviendrait de veiller à ce que seules les personnes dûment autorisées puissent consulter et exporter les données strictement nécessaires à la réalisation des finalités définies par le projet de loi. **Cependant, la CNPD relève que les finalités exactes pour lesquelles ces données seraient consultées ne ressortent pas avec suffisamment de clarté du projet de loi.** Il serait donc pertinent de clarifier ces finalités afin d'assurer que l'accès aux données soit justifié.

50. En effet, la création du registre des certificats de performance énergétique et l'accès audit registre constituent une ingérence dans le droit à la vie privée et à la protection des données personnelles. En vertu du principe de proportionnalité consacré notamment par l'article 52.1 de la Charte des droits fondamentaux de l'Union européenne, une telle ingérence doit être limitée au strict nécessaire[458].

51. En outre, il y a lieu de rappeler l'importance des mesures de sécurité afin de prévenir des accès non-autorisés aux données. Sur ce point, il est renvoyé au titre IV du présent avis.

III. Le cadastre de chaleur

A. Remarques liminaires

52. Le projet de loi prévoit également la création d'un nouveau registre intitulé « cadastre de chaleur » dont l'objectif est de centraliser les données provenant de diverses sources en lien direct avec l'évolution de la consommation de chaleur des immeubles bâtis pour l'ensemble du territoire national. Ces données sont destinées à être affichées dans une application cartographique. À cet égard, la collecte et le traitement de certaines données à caractère personnel, telles que celles relatives à la consommation énergétique et à la performance énergétique des bâtiments, s'avèrent nécessaires.

53. L'article 28.2.1° dispose que le registre de chaleur a notamment pour finalité de servir comme *« outil aux communes sous forme de répertoire cartographique ».* En ce sens, la CNPD comprend que l'objectif principal de ce registre est d'organiser et de structurer les données relatives à la consommation et à la performance énergétique des bâtiments afin de les visualiser de manière claire et intuitive dans une application cartographique. En vue d'améliorer la lisibilité du texte sou avis, la Commission nationale recommande aux auteurs du projet de loi de créer un article distinct dédié spécifiquement aux dispositions relatives à la représentation cartographique. Cette modification permettrait de mieux distinguer le traitement des données concernant la collecte des données de ceux concernant la visualisation desdites informations.

B. Quant au responsable du traitement

54. Selon l'article 28.1 du projet de loi *« [i]l est créé, dans le respect des exigences de la législation en matière de protection*

[458] V. notamment CJUE, arrêt du 22 novembre 2022, WM et Sovim SA contre Luxembourg Business Registers, affaires jointes C-37/20 et C-601/20, points 63 à 65.

de données et de la vie privée un registre dénommé « cadastre de chaleur » qui est déployé par un organisme désigné par le ministre qui assure le rôle de responsable de traitement visé par l'article 4, point 7, du [RGPD]. ». Au vu de l'importance de la notion du responsable du traitement dans l'application du RGPD[459], cette disposition soulève plusieurs interrogations.

55. En effet, il ne ressort pas clairement des dispositions sous avis, quelle entité est à qualifier de responsable du traitement. S'agit-il de l'organisme désigné par le ministre ou du ministre lui-même ? Cela devrait être formulé sans ambiguïté dans le texte du projet de loi. Par ailleurs, si l'organisme traite les données personnelles pour ses propres finalités ou conserve ces données pour le compte du ministre, alors il s'agirait d'une sous-traitance. La notion de sous-traitant est définie par l'article 4.8) du RGPD 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 »*. Dans ce cas, l'établissement d'un contrat de sous-traitance, répondant aux critères de l'article 28 du RGPD, s'avère nécessaire.

56. En outre, il y a lieu de s'interroger sur le fait que cet organisme soit un acteur public ou une entreprise privée. En effet, confier la gestion d'un registre national dans l'intérêt public et le traitement de données y relatif par une loi à une entreprise privée serait contestable. Pour une meilleure compréhension du texte sous avis et afin de respecter le principe de prévisibilité auquel doit répondre tout texte légal ou règlementaire[460], la CNPD estime indispensable de clarifier à la lumière des développements précédents le rôle et la qualité de l'entité en charge du déploiement du registre.

57. La CNPD relève que, dans le cas où un acteur privé aurait accès à un registre public et à des données de consommation, il est nécessaire de préciser de manière explicite que toute réutilisation de ces données à des fins commerciales soit interdite.

58. La CNPD souligne que l'article L.126-32 du code de la construction et de l'habitation français précité[461] prévoit explicitement que *« [l]es informations ne peuvent pas être utilisées à des fins commerciales. »* Elle invite ainsi les auteurs du projet de loi luxembourgeois à s'inspirer de cette disposition, afin d'éviter toute exploitation commerciale.

59. Par ailleurs, en ce qui concerne les dispositions des paragraphes 2 et 3 de l'article 28.6 du projet de loi[462], il convient de réitérer les observations formulées au point 21 du présent avis. Dès lors, l'article

[459] V. point 18 du présent avis.
[460] 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.
[461] V. point 36 du présent avis.
[462] L'article 28.6 dispose que *« [l]e responsable de traitement] n'est responsable que de la sécurisation et du traitement des données dans le registre et de la visualisation de l'historique des traitements des usagers dans le répertoire cadastral. Il n'est pas responsable de l'exactitude et de l'exhaustivité des données importées à partir des bases de données visées au paragraphe 4 ou éditées par les usagers conformément au paragraphe 5 ».*

ANNEXES

28.6 du projet de loi ne devrait pas exclure la responsabilité du ministre quant à l'exactitude et l'exhaustivité des données importées dans le registre.

60. En outre, il y a lieu de préciser que les responsables du traitement qui importent des données à caractère personnel dans le registre sont tenus de garantir la véracité et l'exactitude de ces données. Conformément au principe d'exactitude prévu à l'article 5.1 d) du RGPD, ils doivent veiller à ce que les données personnelles soient non seulement exactes, mais également, le cas échéant, mises à jour. Cette disposition impose également aux responsables du traitement de prendre toutes les mesures raisonnables afin que les données inexactes, au regard des finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

C. Quant aux catégories de données

61. L'article 28.3 dispose que : *« [l]e registre visé au paragraphe 1er comprend, outre les données publiquement accessibles, les données suivantes :*

1° les données contenues dans le calcul de performance énergétique et le certificat de performance énergétique authentifiés telles que visées à l'article 27, paragraphe 3, point 2°, hormis les noms et prénoms des propriétaires ;

2° le nombre d'unités contenues dans un bâtiment ;

3° les données relatives aux demandes d'aides financières pour l'assainissement énergétique et les installations techniques valorisant les sources d'énergie renouvelables telles que visées par la loi modifiée du 23 décembre 2016 instituant un régime d'aide pour la promotion de la durabilité, de l'utilisation rationnelle de l'énergie et des énergies renouvelables dans le domaine du logement concernant le nombre, type et taille des installations, l'année de dépôt de la demande, les coordonnées du demandeur, le type de bâtiment et les indications sur l'alimentation par un réseau de chaleur ;

4° les données relatives au statut de raccordement d'une parcelle cadastrale à un réseau de chaleur ainsi qu'à la production ou la consommation d'énergie thermique des points de raccordement ;

5° les données relatives à la consommation de gaz naturel d'un point de raccordement. »

S'il convient de saluer l'énumération des catégories de données qui seraient collectées, il y a lieu de relever, que le principe de minimisation des données devrait être respecté, de sorte que seules les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités soient traitées[463]. De ce fait, la Commission nationale s'interroge particulièrement sur la nécessité d'intégrer les données relatives aux demandes d'aides financières (3°).

[463] Article 5.1 c) du RGPD.

62. De plus, il y a lieu de constater que le registre comprend notamment des données liées à la consommation en énergie des bâtiments et souligne que ces données sont susceptibles de fournir un aperçu extrêmement détaillé des habitudes des individus. À cet égard, il serait opportun de diminuer la granularité des données, c'est-à-dire de rendre les informations intégrées dans le cadastre plus générales, afin d'exclure tout risque de réidentification des personnes concernées.

63. Par ailleurs, il y a lieu de regretter que les catégories de données visées par le point 1° de la disposition précitée ne soient pas précisées. Il est indiqué qu'un projet de règlement grand-ducal préciserait les données contenues dans le calcul de performance énergétique et le certificat de performance énergétique authentifiés et la CNPD regrette qu'un tel projet de règlement grand-ducal n'ait pas été transmis en même temps que le projet de loi.

D. Quant aux finalités

64. Il y a lieu de relever que l'article 28.2 du projet de loi énumère les finalités du cadastre de chaleur qui sont les suivants :

« 1° de servir d'outil aux communes sous forme de répertoire cartographique dans le cadre de la mise en œuvre des mesures du catalogue du Pacte Climat concernant la planification communale en faveur de l'énergie et du climat en permettant :

a) d'identifier les sources et réseaux de chaleur et de froid existants sur le territoire communal ;

b) d'identifier et de calculer les besoins en chaleur et de froid des bâtiments sur le territoire communal ;

c) de déterminer les zones favorables à l'utilisation d'énergies renouvelables ou de la chaleur et de froid fatals compte tenu de la disponibilité des différentes sources d'énergie ou de chaleur, de l'efficacité énergétique, de l'efficacité et de la durabilité des réseaux de chaleur et de froid ;

d) de quantifier les potentiels de chaleur et de froid fatals et d'énergies renouvelables utilisables ainsi que les potentiels d'efficacité énergétique ;

e) d'établir des bilans énergétiques et la stratégie communale au niveau énergétique et climatique ;

2° d'assurer la conservation des données à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques ;

3° de permettre l'élaboration et la mise à disposition de statistiques et de données agrégées et anonymisées à des fins d'information, de transparence et de recherche. »

Il convient de rappeler que conformément au principe de limitation des finalités[464], les

[464] Article 5.1 b) du RGPD.

ANNEXES

données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne doivent pas, en principe, être traitées pour des finalités « incompatibles » avec ces finalités d'origine.

65. Il ressort de l'article 28.2 du projet de loi que le cadastre de la chaleur ait pour finalité *d'« assurer la conservation des données à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques ».* En ce qui concerne les traitements à des fins statistiques et scientifiques, il est renvoyé aux développements formulés aux points 33 et suivants du présent avis.

E. Quant à l'accès au registre « cadastre de chaleur »

66. L'article 28.5 dispose qu': *« ont accès au répertoire cadastral visé au paragraphe 2, point 1°, des agents communaux individuellement désignés par leur bourgmestre en vue de l'exécution des missions visées au point 1° précité ainsi que des agents publics, nommément désignés par le ministre en fonction de leurs attributions, dans l'exercice de leurs attributions sous l'autorité du ministre. Les usagers visés à l'alinéa 1er ont accès au répertoire cadastral via un accès individuel et sécurisé leur permettant de visualiser et d'éditer les informations concernant le territoire de leur commune. Le répertoire archive les traitements opérés sous forme d'historique visualisant de manière transparente les traitements opérés par les différents usagers. »*

67. La CNPD note que le cadastre de chaleur ne sera pas accessible au public et que seuls les agents des administrations communales ou du ministère pourront y accéder dans le cadre de leurs missions. Au-delà, les usagers, désignés comme tels par les auteurs du projet de loi, pourront accéder au répertoire cadastral via un accès individuel et sécurisé afin de visualiser et d'éditer les informations concernant le territoire de leur commune.

68. Le paragraphe 2 de l'article 28.5 du projet de loi dispose que *« [...] Le répertoire archive les traitements opérés sous forme d'historique visualisant de manière transparente les traitements opérés par les différents usagers. »*. La Commission nationale comprend qu'il s'agit d'une journalisation des accès (registre des logs) afin de pouvoir garantir la traçabilité des accès. Il y a lieu de souligner que la journalisation des accès est soumise comme toutes les données à caractère personnel à une durée de conservation[465]. Ainsi, il est recommandé aux auteurs du projet de loi d'éviter l'utilisation du terme « archive », car celui-ci pourrait prêter à confusion. À cet égard, il est renvoyé aux développements formulés sous le point 76 du présent avis.

IV. <u>Les mesures de sécurité</u>

69. Conformément à l'article 5.1 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*

[465] V. point 70 du présent avis.

perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ».

70. 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. Il y a lieu de rappeler qu'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 concernée, et à quelles données précises cette personne ou ce service aurait accès.

71. 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 proactivement des contrôles en interne. À cet effet, il convient conformément à l'article 32.1 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 ».*

72. La mise en œuvre de ces mesures devrait tenir compte des spécificités de chacun des accès envisagés par le projet de loi.

En effet, les personnes habilitées importent via une plateforme gouvernementale sécurisée qui requiert une authentification forte les données requises dans le registre des certificats de performance énergétique. En ce qui concerne le cadastre de chaleur, les agents communaux individuellement désignées par le bourgmestre ainsi que des agents publics désignés par le ministre et les usagers ont accès au répertoire cadastral via un accès individuel et sécurisé.

73. Par ailleurs, dans le cadre des différents accès envisagés par le projet de loi, le principe de minimisation devrait être respecté, de sorte que seules les données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles seraient traitées soient communiquées.

V. Les durées de conservation

74. Conformément l'article 5.1 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. Or, le projet de loi sous avis ne comporte pas de disposition fixant la durée de conservation des données traitées.

75. En effet, l'article 22.1 du projet de loi dispose qu'*« un certificat de performance énergétique a une validité de dix ans à partir de la date de son authentification. »*. De plus, l'article 24.1 du projet de loi prévoit que *« les personnes visées à l'article 21, paragraphe 3, assurent un archivage d'au moins dix ans des calculs de performance énergétique et des certificats de performance énergétique qu'ils ont établis pour un bâtiment donné. ».*

ANNEXES

La Commission nationale comprend qu'une durée de conservation d'*« au moins dix ans »* implique que cette durée minimale pourrait être prolongée et souligne qu'une telle formulation est contraire à l'article 5.1 e) du RGPD. Il est recommandé aux auteurs du projet de loi de prévoir une durée de conservation précise. Par ailleurs, en l'absence de précisions des auteurs du projet de loi quant à la nécessité d'une conservation de dix ans, 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 et invite les auteurs du projet de loi à fournir des précisions à cet égard.

76. Finalement, la CNPD attire l'attention des auteurs du projet de loi sur l'importance de distinguer entre la durée de conservation des données et leur archivage, deux concepts distincts dans le « cycle de vie » des données personnelles. La durée de conservation correspond à la durée nécessaire à la réalisation de l'objectif ayant justifié la collecte et l'enregistrement des données personnelles. En revanche, l'archivage intervient après que l'objectif du traitement des données a été atteint et lorsque ces données présentent encore un intérêt administratif pour l'organisme (par exemple, pour la gestion d'un éventuel contentieux) ou doivent être conservées pour répondre à une obligation légale[466].

Ainsi adopté à Belvaux
en date du 15 novembre 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[466] V. Guide pratique de la CNIL *« Guide pratique sur les durées de conservation »*, Version juillet 2020, disponible sous : https://www.cnil.fr/sites/cnil/files/atoms/files/guide_durees_de_conservation.pdf, p.4.

6

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°8186A portant modification de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; de la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes, des droits d'accise sur l'eau-de-vie et des cotisations d'assurance sociale ; de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines, de l'Administration des douanes et accises et portant modification de la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée; la loi générale des impôts (« Abgabenordnung ») ; la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes; la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines ; la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale.

Délibération n°69/AV29/2024
du 22 novembre 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. En date du 7 août 2024, la CNPD a avisé[467] le projet de loi n°8186A portant modification de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; de la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes, des droits d'accise sur l'eau-de-vie et des cotisations d'assurance sociale ; de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et

[467] Voir Délibération n°53/AV21/2024 du 7 août 2024 de la Commission nationale pour la protection des données, doc. parl. 8186A/02.

ANNEXES

judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines, de l'Administration des douanes et accises et portant modification de la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée; la loi générale des impôts (« Abgabenordnung ») ; la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes; la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines ; la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale (ci-après le « projet de loi »).

3. Par courrier du 13 novembre 2024, le Ministère des Finances a invité la Commission nationale à se prononcer sur l'amendement parlementaire au projet de loi, adopté par la Commission des Finances lors de sa réunion du 12 novembre 2024 (ci-après l'« amendement parlementaire »).

4. La CNPD note que l'amendement parlementaire vise à reprendre les observations d'ordre légistique proposées par le Conseil d'État dans son avis complémentaire du 22 octobre 2024[468].

Par ailleurs, elle note que les dispositions de l'amendement parlementaire ne soulèvent pas de nouvelles problématiques d'un point de vue de la protection des données, autres que celles relevées dans son avis antérieur. Dès lors, la Commission nationale se permet de réitérer l'ensemble de ses remarques y formulées[469].

Ainsi adopté à Belvaux
en date du 22 novembre 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[468] Voir avis complémentaire n°61.915 du Conseil d'État du 22 octobre 2024, doc. parl. 8186A/03.
[469] Voir Délibération n°53/AV21/2024 du 7 août 2024 de la Commission nationale pour la protection des données, doc. parl. 8186A/02.

6

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet n°8253 relative aux fiches d'hébergement et portant : 1° modification de loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 2° modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ; et 3° abrogation de la loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement

Délibération n°70/AV30/2024
du 6 décembre 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. Conformément à l'article 46.1.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 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, la Commission nationale *« 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 ».*

3. En date du 29 mars 2024, la CNPD a avisé[470] le projet de loi n°8253 relative aux fiches d'hébergement et portant :

[470] V. Délibération n°20/AV8/2024 du 29 mars 2024 de la Commission nationale pour la protection des données, doc. parl. 8253/03.

ANNEXES

1° modification de loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ; 2° modification de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale ; et 3° abrogation de la loi modifiée du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement (ci-après le « projet de loi »).

4. Par courrier du 5 août 2024, le Ministère de l'Économie a invité la Commission nationale à se prononcer sur les amendements parlementaires apportés audit projet de loi (ci-après les « amendements »). La Commission nationale note que les amendements visent essentiellement à donner suite aux oppositions formelles émises par le Conseil d'État dans son avis du 12 décembre 2023[471] et n'ont pas repris les remarques formulées par la CNPD dans son avis initial. Dès lors, dans la mesure où ses observations n'ont pas été suivies et que les modifications envisagées introduisent de nouveaux éléments, la Commission nationale entend réitérer les observations formulées dans son avis précité et émettre des recommandations complémentaires en lien avec les amendements proposés.

XXXV. Sur le fichier des fiches d'hébergement

E. Remarques liminaires

5. Tout d'abord, il convient de rappeler que l'article 6 du projet de loi initial prévoyait une transmission systématique et généralisée des fiches d'hébergement à la Police grand-ducale ainsi qu'à l'Institut national de la statistique et des études économiques du Grand-Duché de Luxembourg (ci-après le « STATEC »).

6. Afin de répondre à l'opposition formelle formulée par le Conseil d'État dans son avis du 12 décembre 2023[472], les auteurs des amendements parlementaires ont supprimé le recours à des fiches d'hébergement sous forme papier, et proposent de consigner, au lieu et place de la transmission directe desdites fiches d'hébergement à la Police grand-ducale et au STATEC, les données figurant sur les fiches d'hébergement dans un fichier des fiches d'hébergement. Dès lors, les nouvelles dispositions à l'article 5.1 du projet de loi entendent créer un fichier des fiches d'hébergement.

F. Sur le responsable du traitement du fichier des fiches d'hébergement

7. Il convient de rappeler que la notion de responsable du traitement joue un rôle important en matière de protection des données et la détermination du responsable du traitement peut avoir des incidences sur le régime juridique applicable[473].

Comme précisé dans l'avis initial de la Commission nationale, l'exploitant[474] est le responsable du traitement pour la collecte

[471] V. Avis du Conseil d'État n°61.524 du 12 décembre 2023, doc. parl. 8253/02.
[472] V. Avis du Conseil d'État n°61.524 du 12 décembre 2023, doc. parl. 8253/02, p.4.
[473] Délibération n°20/AV8/2024 du 29 mars 2024 de la Commission nationale pour la protection des données, doc. parl. 8253/03, point 11.
[474] L'article 1er, 1° du projet de loi définit l'exploitant comme *« toute personne physique ou morale désignée comme exploitant sur la fiche d'hébergement qui fournit, à titre onéreux, un service d'hébergement touristique ».*

et la transmission subséquente des données des voyageurs[475]. Le STATEC, la Police grand-ducale et le Service de renseignement de l'État (ci-après le « SRE ») sont quant à eux à considérer comme des responsables des traitements distincts pour les traitements de données qu'ils effectuent par la suite[476].

8. Cependant, la création du fichier des fiches d'hébergement soulève des interrogations concernant le rôle du ministre ayant le tourisme dans ses attributions (ci-après le « ministre »). En effet, en l'absence de précisions à ce sujet dans les amendements, la Commission nationale se demande si le ministre est bien à qualifier de responsable du traitement dudit fichier[477]. Elle s'interroge plus particulièrement sur le fait de savoir si le ministre exerce un **contrôle effectif** sur la gestion du fichier et s'il peut être considéré comme responsable du traitement au sens de l'article 4.7 du RGPD.

9. Par ailleurs, la CNPD se demande encore si le ministre a la possibilité d'accéder aux données contenues dans le fichier des fiches d'hébergement[478]. Un tel accès serait, aux yeux de la CNPD, difficilement conciliable avec les principes fondamentaux du droit à la protection des données à caractère personnel, en particulier avec les principes de finalité et de minimisation des données, tel que prévu à l'article 5.1 b) et c) du RGPD.

À cet égard, la Commission nationale s'interroge plus particulièrement sur les raisons pour lesquelles le ministre se verrait confier cette mission et regrette que les auteurs des amendements parlementaires n'aient pas précisé les motifs justifiant ce choix. Ce d'autant plus alors que l'article 45.1 point b), de la Convention d'application de l'Accord de Schengen prévoit la possibilité d'une transmission directe aux autorités compétentes[479].

10. Enfin, la tenue d'un tel registre auprès du ministèrere suscite des inquiétudes de la part de la CNPD alors qu'il y a lieu de s'interroger sur la détermination du régime juridique qui serait applicable en l'espèce. En effet, les fiches d'hébergement qui seraient conservées dans ce fichier sont collectées pour des finalités différentes, à savoir :

- Les fins prévues à l'article 43sexies de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale (données transmises à la Police grand-ducale) ;
- Les fins prévues à l'article 5 de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement

[475] Délibération n°20/AV8/2024 du 29 mars 2024 de la Commission nationale pour la protection des données, doc. parl. 8253/03, point 12.
[476] Ibidem.
[477] Art. 1.5 et art. 5.1 du projet de loi.
[478] Comité européen de la protection des données (EDPB), Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, point 45, disponibles sous : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_fr.
[479] Art. 45.1 b) de la Convention d'application de l'Accord de Schengen : *« les fiches de déclaration ainsi remplies seront conservées pour les autorités compétentes ou seront transmises à celles-ci, pour autant que ces autorités le jugent nécessaire pour la prévention de menaces, pour des poursuites pénales ou pour éclaircir le sort de personnes disparues ou victimes d'accidents, sauf si le droit national en dispose autrement. »*

ANNEXES

de l'État, tel que modifié par le projet de loi (données transmises au SRE) ; et
- Les fins prévues à l'article 9 du règlement (UE) no 692/2011 du Parlement européen et du Conseil du 6 juillet 2011 concernant les statistiques européennes sur le tourisme et abrogeant la directive 95/57/CE du Conseil (données transmises au STATEC).

Ainsi, deux régimes juridiques sont susceptibles de s'appliquer l'un découlant de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, et l'autre découlant du RGPD.

G. Sur la transmission systématique et généralisée des fiches d'hébergement

11. Dans son avis initial, la CNPD s'est inquiétée que les données à caractère personnel contenues dans les fiches d'hébergement soient systématiquement transmises aux autorités compétentes, notamment à la Police grand-ducale[480].

12. Ces inquiétudes étaient d'ailleurs partagées par le Conseil d'État, qui a sanctionné cette disposition par une opposition formelle, en relevant que *« la transmission systématique et généralisée des données aboutissant à une surveillance massive et non ciblée de tous les voyageurs constitue une atteinte manifestement disproportionnée par rapport à l'objectif, à savoir la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales par la Police grand-ducale. Selon le Conseil d'État, une telle transmission constitue une ingérence disproportionnée au droit à la protection de la vie privée et au droit à la protection des données à caractère personnel tels que consacrés par les articles 20 et 31 de la Constitution, l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ainsi que l'article 5 du [RGPD] »*[481].

13. Afin de répondre à l'opposition formelle du Conseil d'État, les auteurs des amendements parlementaires ont supprimé le recours à des fiches d'hébergement sous forme papier, et proposé que les données des voyageurs soient dorénavant transmises par les exploitants dans le fichier des fiches d'hébergement.

14. Toutefois, la CNPD estime que ces amendements ne permettent pas de lever les inquiétudes soulevées dans son avis du 29 mars 2024[482]. Elle estime également que ces dispositions constituent toujours une ingérence disproportionnée au droit à la protection de la vie privée et au droit à la protection des données, tel que relevé par le Conseil d'État.

[480] Délibération n°20/AV8/2024 du 29 mars 2024 de la Commission nationale pour la protection des données, doc. parl. 8253/03, points 29 et s.
[481] Avis du Conseil d'État n°61.524 du 12 décembre 2023, doc. parl. 8253/02, p.4.
[482] Délibération n°20/AV8/2024 du 29 mars 2024 de la Commission nationale pour la protection des données, doc. parl. 8253/03.

15. En effet, l'abolition des fiches d'hébergement sous forme papier ne résout pas la problématique de la surveillance massive et non ciblée soulevée par le Conseil d'État[483]. Bien que le texte sous avis ne prévoit plus une transmission directe aux autorités compétentes, les amendements envisagent une transmission des informations par les exploitants vers un fichier centralisé.

Dès lors, la CNPD estime que la création d'une banque de données auprès du ministre, qui tiendrait ces données personnelles à disposition de la Police grand-ducale et du SRE, le cas échéant, n'atténue pas le caractère disproportionné de la transmission de données personnelles des voyageurs.

16. En outre, comme expliqué plus amplement dans l'avis initial de la Commission nationale, la jurisprudence européenne considère la conservation généralisée et indifférenciée des données relatives à la localisation des personnes comme incompatible avec les articles 7 et 8 ainsi qu'avec l'article 52.1 de la Charte des droits fondamentaux de l'Union européenne[484]. Ainsi, les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire[485].

17. De plus, il convient encore de rappeler que la transmission systématique des données personnelles des voyageurs par l'exploitant aux services de police a été abrogée dans tous nos pays voisins[486] et que le système des fiches d'hébergement au Grand-Duché du Luxembourg reste malgré l'abolition des fiches d'hébergement sous forme papier plus intrusif. La CNPD regrette que les auteurs des amendements parlementaires ne se soient pas inspirés du modèle des législations belge et français, comme le recommandait expressément le Conseil d'État[487].

18. Par conséquent, la Commission nationale réitère ses réserves, formulées dans son avis initial, concernant la transmission systématique et généralisée des données aboutissant à une surveillance disproportionnée des personnes concernées.

H. Sur le droit d'accès des membres de la Police grand-ducale et du SRE au fichier des fiches d'hébergement

19. La Commission nationale salue les modifications apportées par l'amendement 12. Cet amendement vise à encadrer l'accès de la Police grand-ducale au fichier des fiches d'hébergement.

20. Ainsi, ces dispositions visent à introduire des règles concernant la traçabilité des accès et la finalité des traitements opérés par les membres de la Police grand-ducale, ainsi qu'une disposition interdisant expressément *« d'utiliser les informations*

[483] Amendement 9 visant l'article 6, paragraphes 1er et 2.
[484] CJUE, arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, points 50 et s.
[485] CJUE, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 130.
[486] V. Délibération n°20/AV8/2024 du 29 mars 2024 de la Commission nationale pour la protection des données, doc. parl. 8253/03, point 9.
[487] Avis du Conseil d'État n°61.524 du 12 décembre 2023, doc. parl. 8253/02, p. 4.

ANNEXES

et données à caractère personnel et les résultats de traitements de telles données à des fins autres que la prévention ou la répression d'infractions terroristes et des formes graves de criminalité »[488].

21. L'article 5.5 du projet de loi, tel qu'amendé, dispose dorénavant que la Police grand-ducale *« ne peut traiter les informations et données à caractère personnel du fichier des fiches d'hébergement du ministère ayant le Tourisme dans ses attributions et le résultat du traitement de ces données qu'à des fins de prévention, de recherche, de constatation et de poursuite des infractions terroristes et des formes graves de criminalité ».*

22. La CNPD accueille favorablement de telles dispositions alors que la Cour de justice de l'Union européenne a précisé, en ce qui concerne la conservation généralisée de données de localisation, que celle-ci peut être tolérée pour la sécurité nationale sous certaines conditions, tandis que pour la lutte contre la criminalité grave, il faut une limitation selon des critères objectifs, non discriminatoires, et plus restrictive encore pour la criminalité simple[489].

23. En outre, il convient de saluer les dispositions de l'amendement 13 qui entendent créer un accès par le SRE au fichier des fiches d'hébergement.

24. Par ailleurs, il y a lieu de souligner que les lois-cadres[490] respectives de la Police grand-ducale et du SRE doivent expressément encadrer l'accès au fichier centralisé des fiches d'hébergement ainsi que le traitement opéré par leurs agents respectifs. Il y a lieu de souligner que des conditions procédurales doivent être mises en place notamment à travers la réalisation d'un contrôle préalable.

25. Enfin, il convient de relever que l'article 5.6 alinéa 2 du projet de loi prévoit que la Police grand-ducale peut enquêter sur d'autres infractions qui seraient détectées à la suite d'un traitement de données et qui ne rentreraient pas dans le champ d'application de la future loi. Or cette disposition semble être en contradiction avec l'article 5.6 alinéa 1er du projet de loi, qui interdit expressément aux membres de la Police grand-ducale d'utiliser les informations et données à caractère personnel et les résultats de traitements de telles données à des fins autres que la prévention ou la répression d'infractions terroristes et des formes graves de criminalité.

XXXVI. <u>Sur la durée de conservation</u>

26. L'amendement 11 prévoit que *« les données à caractère personnel des voyageurs seront supprimées au plus tard six mois après leur enregistrement dans le fichier des fiches d'hébergement [...] ».*

La Commission nationale se félicite que de telles dispositions définissent une durée précise de conservation des données, et

[489] Pour en savoir plus : Délibération n° 28/AV12/2024 du 16 mai 2024 de la Commission nationale pour la protection des données, point 10.
[490] Loi modifiée du 18 juillet 2018 sur la Police grand-ducale, Loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État, Code de procédure pénale.

6

prévoient qu'à l'issue de celle-ci les données doivent être supprimées.

27. Elle exprime toutefois une réserve concernant la notion *« au plus tard »* qui peut prêter à confusion. À cet égard, elle suggère d'utiliser la formulation suivante *« Les données à caractère personnel des voyageurs sont conservées pour une durée de six mois après leur enregistrement dans le fichier des fiches d'hébergement du ministre ayant le Tourisme dans ses attributions. À l'issue de cette période, elles sont automatiquement supprimées ».*

28. Par ailleurs, le nouvel article 6 du projet de loi tel qu'amendé dispose que : *« [l]es fiches d'hébergement sont conservées dans la solution informatique pendant une durée de six mois. À l'issue de cette période de six mois, elles sont automatiquement supprimées. »*

La Commission nationale estime que cette mesure n'est plus nécessaire alors que les fiches d'hébergement électroniques sont désormais conservées dans le fichier des fiches d'hébergement. Dès lors, elle estime que l'article 6 est superfétatoire et que cette disposition devrait être supprimée.

Ainsi adopté à Belvaux
en date du 6 décembre 2024.

La Commission nationale
pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

ANNEXES

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal portant exécution de l'alinéa 2 du paragraphe 22bis de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung »)

Délibération n°71/AV31/2024
du 13 décembre 2024

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après 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 ».*

L'article 36.4 du RGPD dispose que *« [l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement ».*

2. En date du 7 août 2024, la CNPD a rendu un avis[491] sur le projet de loi n°8186A portant modification de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») ; de la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes, des droits d'accise sur l'eau-de-vie et des cotisations d'assurance sociale ; de la loi modifiée du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines, de l'Administration des douanes et accises et portant modification de la loi modifiée du 12 février 1979 concernant la taxe sur la valeur ajoutée; la loi générale des impôts (« Abgabenordnung ») ; la loi modifiée du 17 avril 1964 portant réorganisation de l'Administration des contributions directes; la loi modifiée du 20 mars 1970 portant réorganisation de l'Administration de l'enregistrement et des domaines ; la loi modifiée du 27 novembre 1933 concernant le recouvrement des contributions directes et des cotisations d'assurance sociale (ci-après le « projet de loi »).

3. En parallèle, la Commission nationale a été saisie de quatre projets de règlements grand-ducaux élaborés dans le cadre des dispositions modifiées ou introduites par le

[491] Délibération n°53/AV21/2024 du 7 août 2024 de la Commission nationale pour la protection des données, doc. parl. 8186A/02.

projet de loi, dont le projet de règlement grand-ducal portant exécution de l'alinéa 2 du paragraphe 22bis de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») (ci-après le « projet de règlement grand-ducal »). La CNPD n'a pas pu identifier de questions relatives à la protection des données à caractère personnel et n'a dès lors pas estimé nécessaire de se prononcer sur les projets de règlements grand-ducaux lui soumis[492].

4. Par courrier du 31 octobre 2024, le Ministre des Finances a invité la Commission nationale à se prononcer sur le projet d'amendements gouvernementaux au projet de règlement grand-ducal portant exécution de l'alinéa 2 du paragraphe 22bis de la loi générale des impôts modifiée du 22 mai 1931 (« Abgabenordnung ») (ci-après les « amendements gouvernementaux »).

5. Le projet de règlement a pour objet de déterminer les travaux ponctuels que l'Administration des contributions directes est autorisée à confier à des contractants ainsi qu'à leurs sous-traitants conformément à l'alinéa 2 du paragraphe 22bis de la loi générale des impôts modifiée du 22 mai 1933 (« Abgabenordnung »). Cette possibilité a été introduite par le projet de loi. Ces dispositions ont été commentées par la Commission nationale dans son avis en date du 7 août 2024[493].

6. La CNPD prend acte que les amendements gouvernementaux visent à reprendre principalement les observations d'ordre légistique proposées par le Conseil d'État dans son avis du 21 juillet 2023[494]. Par ailleurs, un nouveau point 6 est ajouté à la liste des travaux selon lequel l'Administration des contributions directes est autorisée à confier à des contractants et sous-traitants successifs, libellé comme suit : *« [l]es travaux effectués par des consultants externes et ayant pour objet de mettre en œuvre un programme de réorganisation et de modernisation concernant la gestion du personnel, l'organisation interne de l'Administration des contributions directes, le processus de digitalisation interne et les relations avec les contribuables ».*

7. Après examen des amendements gouvernementaux, la CNPD considère qu'ils ne soulèvent pas de nouvelles questions relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement de données à caractère personnel. Cependant, il y a lieu de rappeler que l'article 4.8 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 »* et que le traitement de données à caractère personnel effectué par le sous-traitant doit être régi par un contrat ou un autre acte juridique conformément aux exigences de l'article 28 du RGPD[495]. Finalement, le

[492] Délibération n°53/AV21/2024 du 7 août 2024 de la Commission nationale pour la protection des données, doc.parl. 8186A/02, point 6.
[493] Délibération n°53/AV21/2024 du 7 août 2024 de la Commission nationale pour la protection des données, doc.parl. 8186A/02.
[494] Avis du Conseil d'État n° 61.391 du 21 juillet 2023.
[495] Délibération n°53/AV21/2024 du 7 août 2024 de la Commission nationale pour la protection des données, doc.parl. 8186A/02, point 11.

ANNEXES

responsable du traitement ainsi que le sous-traitant doivent mettre en œuvre des mesures techniques et organisationnelles appropriées afin d'éviter des accès non-autorisés aux données, des fuites de données ou des modifications non désirées conformément à l'article 32 du RGPD[496].

Ainsi adopté à Belvaux
en date du 13 décembre 2024.

La Commission nationale
pour la protection des données

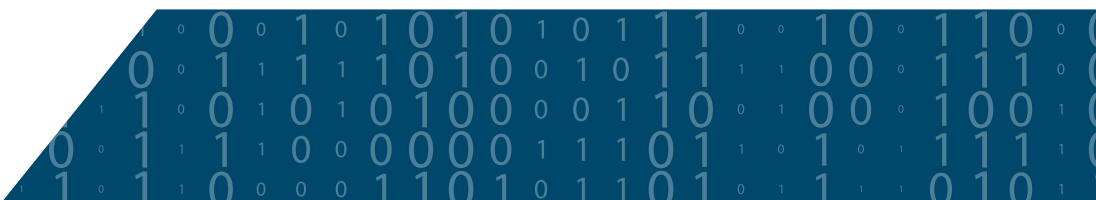
Tine A. Larsen
Présidente

Thierry Lallemang
Commissaire

Marc Lemmer
Commissaire

Alain Herrmann
Commissaire

[496] Ibidem.



brain&more

CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

15, Boulevard du Jazz - L-4370 Belvaux
Téléphone : +352 26 10 60-1
info@cnpd.lu - www.cnpd.lu