RAPPORT ANNUEL 2019


CNPD
COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

INTRODUCTION

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

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

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

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

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

INTRODUCTION

MISSIONS

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

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

Conseiller à travers :
- Les avis relatifs aux projets de loi et aux mesures réglementaires ou administratives concernant le traitement de données personnelles ;
- Les suggestions et recommandations adressées au gouvernement, notamment au sujet des évolutions pertinentes, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et de la communication et des pratiques commerciales ;
- La promotion des bonnes pratiques et la publication de lignes d'orientations thématiques ;
- L'approbation de codes de conduite, des schémas de certification et l'agrément des organismes de certification ;
- Les recommandations au responsable du traitement conformément à la procédure de consultation préalable.

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

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

VALEURS

La CNPD exerce avec **indépendance** les missions qui lui ont été attribuées. Elle détermine ses propres priorités dans les limites de son cadre légal. Elle choisit ses priorités notamment sur base de critères comme la gravité et l'envergure de la violation de la loi et l'étendue des individus affectés.

L'**expertise** est très importante pour la CNPD qui est dédiée à un travail de qualité. A cette fin, la CNPD s'efforce de travailler avec des équipes interdisciplinaires et elle investit dans le développement continu de ses employés pour améliorer leurs connaissances et leurs compétences.

La CNPD assure la **transparence** à l'égard de ses résultats et de ses choix, ce qui génère un support pour son travail et invite au dialogue. La CNPD est ouverte, honnête et visible. Elle promeut une atmosphère positive et ouverte.

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

TABLE DES MATIÈRES

AVANT-PROPOS

1

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

Le 25 mai 2018 était la date d'entrée en application du règlement général sur la protection des données[1], plus communément dénommé le RGPD (ou GDPR - General Data Protection Regulation).

2019 était ainsi la première année complète que la CNPD a travaillé sous l'égide du RGPD et des nouvelles lois nationales de 2018 en matière de protection des données[2].

Pour rappel, le nouveau régime s'applique à tous les acteurs publics et privés – spécifiquement ceux collectant, gérant ou stockant des données à caractère personnel – et vise à cadrer l'usage de ces données, dans le but de :

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

[2] Loi du 1er août 2018 portant organisation de la CNPD et du régime général sur la protection des données et loi du 1er août 2018 relative à la protection des données en matière pénale ainsi qu'en matière de sécurité nationale.

- renforcer le droit des citoyens (droit d'accès, droit à l'oubli, droit à la portabilité, etc.) ;
- responsabiliser davantage les acteurs qui traitent des données personnelles (approche d'« accountability ») et
- uniformiser la réglementation sur la protection des données afin d'établir un cadre harmonisé au sein de l'Union européenne.

Plus d'un an après l'entrée en application du RGPD, les résultats d'un Eurobaromètre spécial[3] de la Commission européenne ont montré que la protection des données était un sujet de préoccupation pour les citoyens européens.

Selon le sondage qui repose sur le point de vue de 27 000 Européens, 73 % des personnes interrogées avaient entendu parler d'au moins un des six droits garantis par le RGPD. En outre, 67 % avaient connaissance du RGPD (71 % au Luxembourg) et 57 % étaient informées de l'existence des autorités nationales chargées de la protection des données. Au Luxembourg, 58 % des personnes interrogées connaissaient la CNPD, soit une augmentation de 25 % par rapport à 2015.

UNE ACTIVITÉ EN HAUSSE

Les nouvelles règles et l'intérêt croissant des particuliers et des professionnels aux enjeux de la protection des données ont conduit à une augmentation des sollicitations de la CNPD.

Tout en restant en-dessous du pic de demandes en 2018, le nombre de sollicitations reste élevé avec 708 demandes de renseignement par écrit en 2019. Alors qu'en 2018, avec l'entrée en application du RGPD, un grand nombre de demandes était en lien avec des questions plus générales relatives à la mise en conformité à la nouvelle législation, les sollicitations sont devenues plus spécifiques, démontrant une plus grande sensibilisation des acteurs en 2019.

Avec 16 avis sur des projets de loi ou mesures réglementaires en lien avec la protection des données, la CNPD a participé activement au processus législatif.

Un des avis les plus marquants de l'année était relatif au fichier central de la Police grand-ducale. Dans le cadre de cet avis, la CNPD s'était nourrie des préoccupations citoyennes, des nombreuses questions parlementaires et des réponses à ces interrogations par les ministres concernés. La CNPD avait également sollicité les autorités de la protection des données d'autres Etats membres au sujet de leur cadre légal en matière de protection des données encadrant les fichiers policiers dans leurs pays. De surcroît, au cours de l'été 2019, la CNPD s'était réunie à plusieurs reprises avec la Police grand-ducale, dans le but d'approfondir sa compréhension de la gestion et l'exploitation qui est faite du fichier central par cette dernière.

[3] https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222

AVANT-PROPOS

1

La CNPD a par ailleurs pris position concernant notamment la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique (VISUPOL), le recours à la vidéosurveillance par les communes, le registre des bénéficiaires effectifs, les associations sans but lucratif et fondations, les annuaires référentiels d'identification des patients et des prestataires ou encore les modalités et conditions de mise en place du dossier de soins partagé.

Le rapport annuel 2019 comprend par ailleurs une partie spéciale sur les traitements de données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale couvrant la période allant du 20 août 2018 au 31 décembre 2019.

GUIDANCE, SENSIBILISATION ET VEILLE SUR DES SUJETS VARIÉS

La CNPD a poursuivi ses efforts de guidance et de sensibilisation en 2019 avec l'élaboration de lignes directrices sur différents sujets comme les conséquences du Brexit en matière de transferts internationaux de données, les campagnes électorales dans le respect de la protection des données ou encore la conformité au RGPD des caméras de vidéosurveillance mobiles destinées à filmer la voie publique (de type « dashcams »).

L'autorité de contrôle a continué à organiser des « DaProLab[4] » après le succès de la première édition en 2018. Les ateliers de travail de 2019 ont porté sur la sécurité des échanges de données entre professionnels du secteur de la santé, les analyses d'impact sur la protection des données, les traitements de données à des fins de recherche scientifique, historique ou statistiques et sur les traitements de données dans le secteur finances/assurances.

À côté des événements qu'elle a organisé elle-même, la Commission nationale a aussi participé à une trentaine de formations, conférences et séminaires pour sensibiliser des publics plus spécialisés aux enjeux de la protection des données.

En outre, la CNPD a commencé à mettre en place une activité de veille technologique et juridique pour suivre des sujets d'innovation comme notamment les nouvelles technologies dans le secteur financier (Fintech), la technologie blockchain et l'intelligence artificielle.

UN NOMBRE RECORD DE RÉCLAMATIONS ET UNE NOUVELLE PROCÉDURE D'ENQUÊTE

Le nombre de réclamations a augmenté considérablement par rapport à l'année précédente, de 450 en 2018 à 625 en 2019.

[4] CNPD's Open Data Protection Laboratory.

Ces réclamations émanent de personnes qui ont fait appel aux services de la CNPD lorsqu'elles ont estimé qu'il y a eu une violation de la loi ou une entrave à l'exercice de leurs droits. Plus d'un quart des réclamations (26%) a été motivé par le non-respect du droit d'accès par les responsables du traitement. Les demandes d'effacement ou de rectification de données auxquelles les suites souhaitées n'avaient pas été réservées ont constitué 21% des réclamations et 11% étaient relatives au droit d'opposition et à la prospection.

En 2019, le CNPD a élaboré un nouveau règlement relatif à la procédure d'enquête qui a été adopté début 2020. Le nouveau règlement tient compte de l'approche double de la CNPD en ce qui concerne les enquêtes. D'un côté, il y a le volet « réactif », largement dirigé par les réclamations, et de l'autre côté le volet « proactif ».

Le nombre d'enquêtes sur place (volet « réactif ») a augmenté de 12 en 2018 à 33 en 2019. Ces enquêtes concernaient notamment les domaines de la vidéosurveillance, de la géolocalisation, de la publicité et du marketing.

Des contrôles « proactifs » ont été effectués sous forme d'audit sur la protection des données. En 2019, la CNPD a poursuivi le travail entamé en 2018 concernant les 25 procédures d'audit thématique sur la fonction de délégué à la protection des données (DPD). La plupart des enquêtes a été clôturée fin 2019 pour être transférée à la Commission nationale siégeant en formation restreinte de décision sur l'issue de l'enquête.

En parallèle à la campagne DPO, 9 audits réactifs ont été ouverts. Il s'agit de plaintes nationales ou issues du mécanisme de coopération européenne pour lesquelles la CNPD a décidé d'ouvrir un audit. Ces plaintes concernent des problématiques variées dont par exemple : le droit d'accès, la sécurité des données, le processus de recrutement ou encore la gestion des cookies, par exemple.

526 VIOLATIONS DE DONNÉES DEPUIS L'ENTRÉE EN APPLICATION DU RGPD

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

En 2019, 354 violations de données ont été notifiées à la CNPD. Au total, la CNPD a reçu 526 violations de données depuis le 25 mai 2018, soit 28 notifications par mois. Comme pour 2018, la principale cause reste l'erreur humaine. Pour y remédier, les responsables de traitement et sous-traitants doivent surveiller d'avantage le facteur humain. Cela passe avant tout par la sensibilisation et la formation du personnel qui doit être systématique et régulière.

AVANT-PROPOS

1

CNPD : RÉORGANISATION DES SERVICES ET ADAPTATION DE L'ORGANIGRAMME

Au cours de l'année 2019, la CNPD a réorganisé ses services et a adapté son organigramme afin de mieux pouvoir assurer ses missions et de faciliter la lisibilité de ses activités.

Il s'agit plus particulièrement des services « Sensibilisation », « Guidance », « Conformité », « Réclamations », « Enquêtes » et « Administration ». Par ailleurs ont été définies les fonctions suivantes directement attachées à la Commission nationale : le(s) secrétaire(s) du collège, le chargé aux relations européennes et internationales et le délégué à la protection des données.

L'année 2019 était également marquée par la préparation à un changement de locaux. Les travaux de planification ont débuté en été pour permettre un déménagement de la CNPD dans le nouveau bâtiment NAOS à Esch-Belval en 2020.

PERSPECTIVES

Au moment de finaliser la rédaction de ce rapport, des évènements exceptionnels ayant marqués jusque-là l'année 2020 montrent à quel point la protection des données personnelles est devenue un sujet fondamental dans la vie sociétale, économique et politique, et ce à un niveau aussi bien global que local.

En particulier la crise sanitaire liée au virus *SARS-CoV-2 (COVID-19)* a créé des défis à court et à long terme sans précédent pour les acteurs publics et privés. Les données à caractère personnel, notamment les données de santé, sont au cœur des problématiques liées à la pandémie. Les États doivent faire face à cette nouvelle menace tout en veillant au respect de la démocratie, de l'État de droit et des droits de l'homme, y compris des droits au respect de la vie privée et à la protection des données. Le RGPD s'est révélé être un outil souple à l'appui de l'élaboration de solutions numériques dans des circonstances imprévues telles que celles-ci et la CNPD s'efforce d'accompagner tous les acteurs dans ce contexte, qu'il s'agisse de professionnels, de particuliers ou du gouvernement.

Sur un autre plan, la Cour de justice de l'Union européenne (CJUE) a invalidé la décision d'exécution relative au « Privacy Shield » en juillet 2020 dans l'affaire *Data Protection Commissioner contre Facebook Ireland et Maximillian Schrems* (Schrems II) sur l'adéquation du niveau de protection des données personnelles offert par les États-Unies dans le cadre de transferts de données vers ce pays. En revanche, la Cour a jugé que la décision de la Commission européenne relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis

Le siège de la CNPD à Belval

dans des pays tiers restait, en principe, valide. Dans le même temps, elle a souligné que ces clauses contractuelles imposent une obligation pour l'exportateur des données et le destinataire du transfert de vérifier, au préalable, que ce niveau de protection est respecté dans le pays tiers concerné, au besoin en mettant en place des garanties supplémentaires. A défaut, les acteurs luxembourgeois et européens doivent suspendre leurs transferts de données et/ou résilier les contrats conclus avec les destinataires des données situés dans des pays tiers. Cet arrêt constitue un évènement clé qui aura donc un impact considérable sur les acteurs luxembourgeois et mobilisera la CNPD et ses homologues européens via le mécanisme de coopération.

Les investissements réalisés par la CNPD en 2019 pour le développement de son organisation, le recrutement de nouveaux collaborateurs et la collaboration avec ses collègues au niveau européens et international permettront à la Commission nationale de continuer à assurer sa mission et à atteindre ses objectifs pendant l'année en cours et dans les années à venir.

Luxembourg, le 6 août 2020

La Commission nationale pour la protection des données

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

L'ANNÉE 2019 EN UN COUP D'ŒIL

2

JANVIER

18 • La CNPD publie des lignes directrices concernant les conséquences du Brexit en matière de transferts internationaux de données.

22-23 • La CNPD participe au Forum International de la Cybersécurité en tant que partenaire.

28 • 13e Journée de la protection des données.

28 • La CNPD participe au Data Privacy Day organisé par Restena et l'Université du Luxembourg.

28 • La CNPD donne une présentation sur « Le rôle de la CNPD à l'ère du nouveau règlement général sur la protection des données » à la Cour de justice de l'Union européenne.

FÉVRIER

13 • La CNPD organise le deuxième DaProLab sur la sécurité des échanges de données entre professionnels du secteur de la santé ainsi qu'entre les professionnels et les patients.

MARS

6 • La CNPD élabore une liste de traitements pour lesquels une analyse d'impact sur la protection des données est obligatoire.

8 • Nominations de Monsieur Marc Lemmer en tant que commissaire et de Madame Martine Kraus en tant que membre suppléant du collège de la CNPD.

AVRIL

19 • La CNPD publie des lignes directrices sur « les campagnes électorales dans le respect de la protection des données personnelles ».

26 • La CNPD organise le troisième DaProLab portant sur les retours d'expérience concernant les AIPD (Analyses d'Impact sur la Protection des Données).

MAI

1 • Marc Lemmer rejoint la CNPD comme commissaire à la protection des données.

6 • La CNPD a participé aux Data Protection Days avec une présentation « RGPD, un an après - quel bilan ? ».

22 • La CNPD publie un avis relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique et un avis relatif au recours à la vidéosurveillance par les communes.

JUILLET

3 • La CNPD organise la quatrième édition du DaProLab sur le thème de « la mise en œuvre de la protection des données pour les traitements à des fins de recherche scientifique ou historique ou à des fins statistiques ».

SEPTEMBRE

13 • La CNPD émet un avis relatif au fichier central de la Police grand-ducale au regard de la législation sur la protection des données.

OCTOBRE

4 • La CNPD organise le cinquième DaProLab sur le thème « Impacts sur les individus pour les traitements de données dans le secteur Finances / Assurances ».

21-24 • La CNPD participe à la 41e conférence internationale des commissaires de la protection des données à Tirana (Albanie).

NOVEMBRE

4-6 • La CNPD participe au Web Summit à Lisbonne.

15 • La Conférence internationale des commissaires de la protection des données a changé son nom en « Global Privacy Assembly (GPA) ».

15 • La CNPD publie une guidance relative à l'utilisation de « dashcams ».

DÉCEMBRE

10 • Journée internationale des Droits de l'Homme.

16 • La CNPD participe à la conférence « La Défense des droits et libertés au Grand-Duché de Luxembourg » à l'Université de Luxembourg.

L'ANNÉE 2019 EN UN COUP D'ŒIL

2

SENSIBILISATION, GUIDANCE ET CONSEIL

3.000

BROCHURES DISTRIBUÉES

lors de la Journée de la protection des données le 28 janvier 2019

36

PRÉSENTATIONS

lors de conférences, séminaires et tables rondes

4

DAPROLABS

Evénement permettant l'échange de vue sur un sujet spécifique entre professionnels de la protection des données

Sujets abordés :
- Sécurité des échanges de données entre professionnels du secteur de la santé
- Analyses d'Impact sur la Protection des Données (AIPD)
- Traitements à des fins de recherche scientifique, historique ou statistiques
- Traitements de données dans le secteur de la finance et des assurances

3

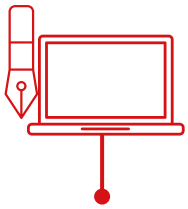
NOUVELLES GUIDANCES

- Lignes directrices sur les conséquences du Brexit en matière de transferts internationaux de données
- Les campagnes électorales dans le respect de la protection des données
- L'utilisation des caméras de vidéosurveillance mobiles destinées à filmer la voie publique (de type « dashcams ») est-elle conforme au RGPD ?

16

AVIS

relatifs à des projets ou propositions de loi ou mesures réglementaires, dont notamment de avis sur :
- le fichier central de la Police
- la vidéosurveillance des espaces et lieux publics
- le recours à la vidéosurveillance par le communes

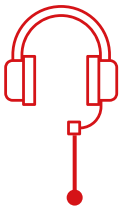


708

DEMANDES DE RENSEIGNEMENT PAR ÉCRIT

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

CONFORMITÉ ET CONTRÔLE

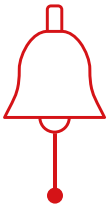


625

RÉCLAMATIONS

Raisons principales :
1. Non-respect du droit d'accès (26 %)
2. Demande d'effacement ou de rectification non respectée (21 %)
3. Droit d'opposition et prospection (11 %)

+ 39 % par rapport à 2018



354

NOTIFICATIONS DE VIOLATIONS DE DONNÉES

Cause principale :
erreur humaine (63 %)

Nature des incidents :
1. données personnelles envoyées au mauvais destinataire (34 %)
2. piratage, hacking (15 %)
3. divulgation des données personnelles à la mauvaise personne (12 %)

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

25

AUDITS « PROACTIFS »

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

entamées en 2018

9

AUDITS « RÉACTIFS »

Il s'agit de réactions à des plaintes concernant des problématiques variées : le droit d'accès, la sécurité des données, le processus de recrutement, la gestion des cookies, etc.

33

ENQUÊTES SUR PLACE

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

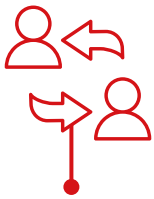
contre 12 en 2018

731

DÉLÉGUÉS À LA PROTECTION DES DONNÉES (DPO)

personnes physiques ou morales déclarées auprès de la CNPD

dont 238 en 2019



1090

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

dont 272 en 2019

LES ACTIVITÉS EN 2019

3

1 SENSIBILISATION, GUIDANCE ET CONSEIL

1.1 ACTIONS DE SENSIBILISATION

28 JANVIER 2019 : 13ÈME JOURNÉE DE LA PROTECTION DES DONNÉES

Le Conseil de l'Europe, avec le soutien de la Commission européenne, a proclamé solennellement le 28 janvier de chaque année comme « Journée de la protection des données ». Le but est de sensibiliser les citoyens sur l'importance de la protection de leurs données personnelles et du respect de leurs libertés et droits fondamentaux, en particulier de leur vie privée.

Pourquoi le 28 janvier ? C'est la date de l'ouverture à la signature de la « Convention 108 » du Conseil de l'Europe (28 janvier 1981). Cette dernière a été le premier instrument international juridiquement contraignant en la matière. Depuis 38 ans, la convention vise à protéger toute personne physique contre l'utilisation abusive des données qui la concernent et à assurer la transparence quant aux fichiers et traitements des données personnelles.

DISTRIBUTION DE LA BROCHURE « VOS DONNÉES ? VOS DROITS ! »

Dans le cadre de la 13ème Journée de la protection des données, la CNPD a distribué sa brochure de sensibilisation du grand public à des endroits stratégiques au Luxembourg (Luxembourg-Gare, Lycées au Limpertsberg et Glacis).

Le but de cette publication intitulée « Vos données ? Vos droits ! » est de présenter les droits des citoyens en matière de protection des données et d'expliquer comment les faire valoir.

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

INTERVENTIONS LORS DU « DATA PRIVACY DAY » ET AUPRÈS DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE

La CNPD a également participé à deux événements à l'occasion de la Journée de la protection des données avec :

- une présentation sur « Le rôle de la CNPD à l'ère du nouveau règlement général sur la protection des données » donnée au personnel de la Cour de justice de l'Union européenne ; et
- une intervention au « Data Privacy Day », organisé par l'Université du Luxembourg et Restena, sur le thème de l'impact des violations des données sur les droits des citoyens.

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

1.2 ORGANISATION DE FORMATIONS ET CONFÉRENCES

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

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

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

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

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

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

B) DAPROLAB

En 2019, la CNPD a continué à organiser des « DaProLab (CNPD's Open Data Protection Laboratory) » après le succès de la première édition en 2018.

Qu'est-ce que le DaProLab ?

- Un atelier de travail où un seul sujet spécifique défini à l'avance est discuté avec comme objectif l'échange d'idées, d'interprétations, de points de vue sur ce sujet entre professionnels de la protection des données.
- Dans le cadre de leur responsabilisation (« accountability »), les participants peuvent confronter leurs décisions, prises de positions, points de vue, idées, pratiques avec les autres participants afin d'obtenir un feedback quant à leurs choix effectués.
- Des échanges de connaissances, d'expériences et de bonnes pratiques.

Le deuxième DaProLab a eu lieu le 13 février 2019 et a porté sur la sécurité des échanges de données entre professionnels du secteur de la santé (secteur hospitalier, cabinets médicaux, pharmacies, laboratoires, entités publiques …) ainsi qu'entre professionnels et patients.

Dans le cadre de cette session ont été abordés :
- les risques liés aux échanges (y compris les risques liés à l'identification des destinataires) ;
- la sécurité technique des échanges ;
- les canaux de communications ;
- les échanges entre professionnels et les échanges entre professionnels et patients.

Le troisième DaProLab a eu lieu le 26 avril 2019 et a porté sur le thème « retours d'expérience sur les AIPD - Analyse d'Impact sur la Protection des Données / Data Protection Impact Assessment (DPIA) ».
Le programme de la session était le suivant :
- rappel sur les AIPD par la CNPD ;
- partage de retours d'expérience : présentations / réalisations par 3 acteurs (IGSS ; LuxGap ; GRC Luxembourg) ;
- échanges et discussion.

La quatrième édition a eu lieu le 3 juillet 2019 et a porté sur le thème de « la mise en œuvre de la protection des données pour les traitements à des fins de recherche scientifique ou historique ou à des fins statistiques ».

Dans le cadre de cette session, les sujets suivants ont été abordés :
- mise en place d'une culture « protection des données » au sein des organisations : bonnes pratiques et difficultés ;
- mise en œuvre des AIPDs dans le monde de la recherche : difficultés liées à l'identification des responsabilités ;

- partage de retours d'expérience ;
- échanges et discussion.

Le cinquième DaProLab a eu lieu le 4 octobre 2019 sur le thème « Impacts sur les individus pour les traitements de données dans le secteur Finances / Assurances ».

Les sujets suivants ont été abordés :
- évaluation des impacts sur les individus des traitements dans les cadre des AIPDs ;
- évaluation des impacts sur les individus dans le cadre de violations de données ;
- les discussions ont notamment porté sur les difficultés à évaluer les impacts sur les individus en raison du manque d'historique, de bases de connaissance, de retours d'expérience réelles.

C) AUTRES ÉVÉNEMENTS AUXQUELS LA CNPD A PARTICIPÉ

À côté des événements qu'elle a organisé elle-même, la Commission nationale a aussi participé à des formations, conférences et séminaires pour sensibiliser des publics plus spécialisés aux enjeux de la protection des données. L'autorité de contrôle est intervenue régulièrement lors de formations récurrentes auprès:
- de l'École Supérieure de Travail (EST) et de l'INAP pour des formations générales sur la protection des données ;
- de Luxinnovation lors d'une session Fit4Start avec un exposé intitulé « What does GDPR mean to my start-up? » ;
- de la confédération luxembourgeoise de commerce (clc) lors d'un atelier de travail animé intitulé « L'écosystème RGPD d'une TPE/PME » ;
- de la Chambre des Salariés (CSL) avec une présentation sur la documentation pour respecter le principe de la responsabilité (« accountability ») et sur le cadre légal de la protection des données personnelles ;
- de l'Ordre des Architectes et Ingénieurs-Conseils (OAI) en collaboration avec la House of Training de la Chambre de Commerce avec une présentation intitulée « Règlement général sur la protection des données : principes et cas pratiques ».

Des présentations axées sur les missions et pouvoirs de la CNPD ont par ailleurs été données lors de l'ERA (Academy of European Law) Summer Course on European Data Protection Law et à la Chambre des Salariés.

Le nouveau règlement général sur la protection des données
En 2019, la CNPD a participé à de nombreux événements en lien avec les nouvelles règles en matière de protection des données afin de sensibiliser le maximum de personnes.

Des présentations plus générales concernant la conformité au RGPD ont notamment été données au Service National de la Jeunesse (SNJ) et à l'Asbl Foyers Seniors.

LES ACTIVITÉS EN 2019

3

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

- à la 11ème édition du Forum International de la Cybersécurité à Lille qui a réuni près de 10 000 participants. La CNPD a partagé son retour d'expérience lors de la table ronde « Le RGPD a un an : quel bilan ? ». Les discussions ont porté notamment sur le bilan en chiffres depuis l'entrée en vigueur du RGPD, les succès et les difficultés pour les organisations privées et publiques à se conformer au RGPD ; la sensibilisation du grand public sur l'exercice de leurs droits en matière de protection des données ; l'exercice de la fonction de DPO et son intégration au sein des organisations et sur la collaboration des autorités de protection des données au sein du comité européen ;
- à la 12ème édition de la conférence « CPDP2019 Computers, Privacy and Data Protection conference » à Bruxelles. La thématique des trois jours de conférence portait sur la protection des données et la démocratie. A cette occasion, la CNPD a participé à la table ronde « AI governance: role of legislators, tech companies and standards bodies » organisée par le centre interdisciplinaire SnT de l'Université du Luxembourg. La CNPD y a présenté son point de vue concernant la gouvernance requise, à différents niveaux, par l'application des exigences de la régulation sur la protection des données aux traitements basés sur des techniques d'intelligence artificielle et les défis auxquels tous les acteurs concernés font face dans ce contexte.
- à la conférence « RGPD : 1 an après… Venez échanger avec la CNPD ! » organisée par la confédération luxembourgeoise du commerce (clc) ;
- aux Luxembourg Data Protection Days avec la présentation intitulée « Partage d'expériences: Recommandations pratiques après un an de RGPD ? » ;
- à l'European Data Privacy Congress organisé par l'Étude Dury Rechtsanwälte avec un exposé intitulé « One Year into GDPR from the regulators' perspective » ;
- au Ferrero Global Privacy Workshop avec l'exposé « One Year into GDPR : the emergence of a global standard ? » ;
- lors d'une conférence organisée par IFE sur les premiers retours d'expérience de la CNPD concernant le RGPD.

Autres thématiques

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

- la certification et le schéma de certification de la CNPD « GDPR Carpa » auprès d'Ernst & Young ;
- le thème « Artificial Intelligence and Data Privacy » auprès de l'ABBL ;
- la protection des données dans le cadre de la recherche généalogique auprès de Aalt Stadhaus à Differdange ;
- la règlementation Blockchain et la gouvernance en Europe lors d'une table ronde organisée par Infrachain asbl ;
- les violations de données dans le secteur financier lors d'une conférence organisée par l'ABBL ;
- le traitement de données personnelles à des fins archivistiques dans l'intérêt public dans le respect de la protection des données à la Journée des Archivistes ;
- audits et investigations de la CNPD lors de la Cyber Security Week ;

- la thématique « Protecting the right to privacy and data protection in a society of risks » au séminaire intitulé « Human Rights insights – Data protection » à L'Université du Luxembourg ;
- les nouvelles technologies digitales, l'innovation et les startups, au Web Summit à Lisbonne dans le cadre d'une visite organisée par la Chambre de Commerce du Luxembourg et son Enterprise Europe Network, en collaboration avec la House of Startups, le LOIC et Luxinnovation.

D) LE « GDPR COMPLIANCE SUPPORT TOOL »

Afin d'aider les organisations dans leurs efforts de mise en conformité, la CNPD a développé en 2018 un outil leur permettant de vérifier le niveau de maturité en matière de protection des données : le « GDPR Compliance Support Tool » (CST), disponible à l'adresse https://cst.cnpd.lu. Cet outil a connu en 2019 un intérêt continu avec environ 2000 organisations enregistrées comme utilisateur ce qui correspond à une progression de plus de 11 % par rapport à l'année précédente.

Plusieurs workshops s'adressant principalement aux utilisateurs de cet outil avaient été organisés en 2018. Les objectifs de ces événements étaient :

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

1.3 PARTICIPATION AUX TRAVAUX DE DIFFÉRENTES COMMISSIONS ET RÉSEAUX

La Commission nationale est aussi intervenue périodiquement dans les travaux de

- la Commission Consultative des Droits de l'Homme (CCDH),
- la Commission du registre national des personnes physiques et du
- Comité des statistiques publiques

En 2019, la CNPD a participé aux travaux du « réseau de coopération électorale ». Dans le cadre de la participation de la CNPD à ce réseau, la CNPD a adressé des lignes directrices concernant les campagnes électorales dans le respect de la protection des données personnelles aux acteurs politiques.

Le réseau national de coopération électorale, mis en place sous l'égide du Ministère d'État, est la concrétisation du paquet européen de mesures visant à garantir des élections libres et équitables lancé en septembre 2018. Ce

paquet européen comprend notamment des orientations de la Commission européenne relatives à l'application du droit de l'UE en matière de protection des données dans le contexte électoral ainsi qu'une recommandation de la Commission européenne sur les réseaux de coopération électorale, la transparence en ligne, la protection contre les incidents de cybersécurité et la lutte contre les campagnes de désinformation à l'occasion des élections au Parlement européen.

Finalement, la CNPD a encore participé au comité de suivi de la mise en œuvre des recommandations de la CNPD concernant le fichier central de la Police Grand Ducale (cf. Point 1.5.a) du présent rapport pour plus de détails.

1.4 ÉLABORATION DE GUIDANCES

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

Lignes directrices sur les conséquences du Brexit en matière de transferts internationaux de données
La CNPD a publié des lignes directrices concernant les conséquences du Brexit en matière de transferts internationaux de données. Ces lignes directrices sont destinées à guider les entreprises, organismes publics et associations luxembourgeoises qui sont amenés à transférer des données à caractère personnel vers le Royaume-Uni et qui entendraient poursuivre de tels transferts après le 31 janvier 2020.

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

Les cas de figure suivants sont traités dans le dossier thématique :
1. Transferts au sein de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande)
2. Transferts vers un pays en dehors de l'Espace économique européen disposant d'un niveau de protection adéquat
3. Transferts vers un pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat
4. La coopération internationale en matière policière et judiciaire
5. Les conséquences du Brexit en matière de transferts internationaux de données

Les campagnes électorales dans le respect de la protection des données
La CNPD a publié des lignes directrices concernant « les campagnes électorales dans le respect de la protection des données personnelles ».

En vue des élections européennes qui avaient eu lieu le 26 mai 2019 et à la lumière des révélations sur les phénomènes de désinformation et de manipulation des élections américaines de 2016 et du référendum britannique

sur le Brexit en 2017, la CNPD a souhaité sensibiliser les acteurs politiques sur les risques liés en particulier à la collecte et au traitement des données à caractère personnel des électeurs à des fins électorales.

Dans sa guidance, la CNPD a également émis des recommandations et a exposé les bonnes pratiques en matière de campagnes électorales numériques dans le respect de la protection des données personnelles.

L'utilisation des caméras de vidéosurveillance mobiles destinées à filmer la voie publique (de type « dashcams ») est-elle conforme au RGPD ?
La CNPD se voit régulièrement saisi de demandes de renseignements relatives à des caméras de vidéosurveillance mobiles installées dans les voitures de particuliers, sur des vélos, des motos, ou encore fixées sur les casques de cyclistes, de motocyclistes…

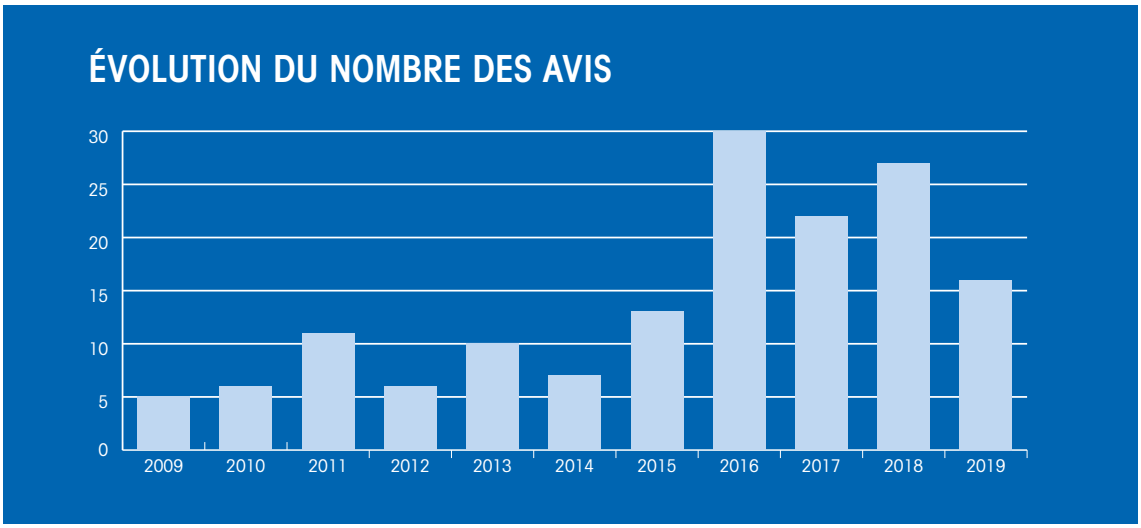
Dans sa guidance à ce sujet, la CNPD a tenu à rappeler qu'elle estime que l'utilisation de telles caméras (parfois appelées « dashcams », à ne pas confondre avec les dispositifs installés dans les voitures aidant le conducteur

à se garer et qui n'enregistrent pas les images) qui filment la voie publique et qui sont susceptibles de capter des images de personnes reconnaissables est en pratique très difficilement réconciliable avec les obligations issues du règlement général pour la protection des données.

1.5 AVIS

Conformément à l'article 57, paragraphe 1er, lettre (e) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la CNPD « conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».

En 2019, la Commission nationale a émis 16 avis sur des projets de loi ou de règlements grand-ducaux. Les avis relatifs aux traitements de données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont résumés dans la partie 2.9.b). Tous les avis peuvent être consultés sur le site Internet de la CNPD à l'adresse https://cnpd.public.lu/fr/publications/rapports/index.html.



A) REGISTRE DES BÉNÉFICIAIRES EFFECTIFS

Le 4 février 2019, la CNPD a avisé le projet de règlement grand-ducal portant exécution de la loi du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs.

La CNPD a commenté l'amendement concernant l'article 5 du projet de règlement grand-ducal, plus précisément les pièces justificatives qui doivent accompagner la demande d'inscription. Suite à l'amendement, les entités immatriculées ne seront plus obligées de transmettre une copie de la pièce d'identité des personnes concernées, dont les données seraient conservées par le registre des bénéficiaires effectifs, si ces dernières disposent d'un numéro d'identification tel que prévu par la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques. Cet amendement vise ainsi à adresser les remarques faites par la CNPD dans son avis du 22 novembre 2018 relatif au projet de loi n°7217 (délibération n°485/2018). Or, une pièce d'identité doit être fournie pour les personnes concernées ne disposant pas d'un tel numéro d'identification. Le commentaire de l'amendement n'adresse pas les interrogations de la CNPD relatives à la nécessité en général de l'obtention et de la conservation de cette pièce d'identité. Selon l'avis de la CNPD, il conviendrait dès lors de le préciser.

Par ailleurs, la CNPD a regretté que les auteurs du projet de règlement grand-ducal n'ont pas jugé opportun de modifier d'autres dispositions du texte, notamment celles concernant les données à caractère personnel figurant au registre (cf. sections II et IV. de l'avis de la CNPD du 22 novembre 2018), les modalités d'accès au registre, y compris l'acquittement des frais, les modalités de recherche, les mesures de sécurité et les mesures visant à prévenir des abus (cf. section V. de l'avis de la CNPD du 22 novembre 2018), ainsi que la durée de conservation des données (cf. section VI. de l'avis de la CNPD du 22 novembre 2018).

B) COMPTES INACTIFS, COFFRES-FORTS INACTIFS ET CONTRATS D'ASSURANCE EN DÉSHÉRENCE

Le 1er février 2019, la CNPD a avisé le projet de loi n°7348 relatif aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence et modifiant : 1. la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et 2. la loi modifiée du 7 décembre 2015 sur le secteur des assurances.

Selon l'exposé des motifs, le projet de loi vise à instaurer en droit luxembourgeois un cadre légal régissant les comptes et coffres-forts inactifs et les contrats d'assurance tombés en déshérence. Il instaure l'obligation pour les établissements de crédit, tel que défini à l'article 1er, point 8. du projet de loi, et les entreprises d'assurance de maintenir un contact régulier avec leurs clients et de les contacter et, si nécessaire, d'entreprendre des recherches complémentaires en cas d'absence de manifestation de la part des clients. Pour le cas où l'inactivité du client se poursuit jusqu'au délai fixé dans le projet de loi, les établissements et entreprises d'assurance devraient consigner les avoirs des clients auprès de la Caisse de consignation.

LES ACTIVITÉS EN 2019

3

Le projet de loi encadre encore les missions des acteurs chargés de veiller à l'application du projet de loi, à savoir la Commission de surveillance du secteur financier (« la CSSF »), le Commissariat aux assurances (« le CAA »), l'Administration des contributions directes (« l'ACD ») et la Caisse de consignation.

La Commission nationale a limité ses observations aux questions soulevées par les dispositions du projet de loi sous examen traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel. Elle a abordé les problématiques des

- traitements de données à caractère personnel effectués par les établissements et les entreprises d'assurances ;
- traitements de données à caractère personnel effectués par la Caisse de consignation, la CSSF, le CAA et l'ACD ; et des
- droits des personnes concernées.

Dans son avis, la CNPD a recommandé notamment :

- de préciser davantage le projet de loi en ce qui concerne la durée de conservation des données ;
- de prévoir de manière plus précise dans le corps du texte de l'article 32 le contenu du registre tenu par la Caisse de consignation. ;
- d'encadrer la coopération des organismes publics dans le projet de loi, en indiquant les données susceptibles d'être échangées et
- que le responsable de traitement procède à une information claire et complète sur son site internet comportant les informations requises en vertu de l'article 14 du RGPD.

C) LIMITATION DE LA PORTÉE DE CERTAINS DROITS ET OBLIGATIONS DANS LE CADRE DU RGPD

Le 5 avril 2019, la CNPD a avisé le projet de loi n°7373 concernant la limitation de la portée de certains droits et obligations dans le cadre du règlement général sur la protection des données et portant : 1. mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ; 2. modification de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et 3. modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances.

Selon l'exposé des motifs, ce projet de loi entend modifier la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier et la loi modifiée du 7 décembre 2015 sur le secteur des assurances afin de permettre à la Commission de surveillance du secteur financier (ci-après « la CSSF ») et au Commissariat aux Assurances (ci-après « le CAA ») de se prévaloir de certaines des limitations énoncées à l'article 23, paragraphe 2 du RGPD dans l'accomplissement de leurs missions.

Ayant déjà été consultée par le ministère des Finances au stade d'avant-projet de loi en question, la Commission nationale s'est limitée à formuler les observations sur les problématiques suivantes :

- les données traitées par la CSSF (article 16-1 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-1 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi) ;
- le traitement à une fin autre que celle pour laquelle les données ont été collectées par la CSSF (article 16-2 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-2 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi) ;
- la limitation du droit à l'information par la CSSF (articles 16-3 et 16-4 de la loi modifiée du 23 décembre 1998, tels qu'insérés par le projet de loi) et par le CAA (articles 13-3 et 13-4 de la loi modifiée du 7 décembre 2015, tels qu'insérés par le projet de loi) ;

- la limitation du droit d'accès par la CSSF (article 16-5 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-5 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi) ;
- la limitation du droit à la limitation du traitement par la CSSF (article 16-6 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-6 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi) ;
- la limitation du droit de s'opposer au traitement par la CSSF (article 16-7 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-7 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi) ;
- les garanties (articles 16-8 et 16-9 de la loi modifiée du 23 décembre 1998, tels qu'insérés par le projet de loi, et articles 13-8 et 13-9 de loi modifiée du 7 décembre 2015, tels qu'insérés par le projet de loi).

D) PLATEFORME ÉLECTRONIQUE SÉCURISÉE SERVANT AUX AUTORITÉS JUDICIAIRES ET AU SRE

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.

Il résulte de l'exposé des motifs que le projet de loi analysé vise à mettre en place une plateforme commune et unique de transmission électronique sécurisée servant aux autorités judiciaires ainsi qu'au Service de renseignement de l'État. Selon les auteurs du projet de loi, la plateforme offre une protection accrue des données personnelles des personnes faisant l'objet de mesures de repérage, de surveillance ou de contrôle.

La Commission nationale a toutefois constaté dans son avis que le projet de loi reste muet sur les mesures techniques et organisationnelles à mettre en place pour garantir un niveau de sécurité adapté au regard de la sensibilité des données transmises via la plateforme, d'autant plus que le titre du projet de loi annonce la création d'une plateforme électronique « sécurisée ». De plus, elle a regretté que le projet de règlement grand-ducal qui est censé définir le format et les modalités d'exécution suivant lesquelles les données collectées sont à transmettre respectivement aux autorités judiciaires et au Service de renseignement de l'Etat n'a pas été annexé au projet de loi.

Dans son avis, la CNPD a formulé des commentaires et réflexions sur le champ d'application, les définitions, la plateforme commune de transmission électronique sécurisée et la modification du Code de procédure pénale et de l'article 7, paragraphe 3, alinéa 1, de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

E) ASSOCIATIONS SANS BUT LUCRATIF ET FONDATIONS

Le 18 juin 2019, la Commission nationale s'est autosaisie pour aviser le projet de loi n°6054 sur les associations sans but lucratif et les fondations, ainsi que la proposition de loi n°7392 portant modification de la loi modifiée du 21 avril 1928 sur les associations et les fondations sans but lucratif.

A titre préliminaire, la CNPD a abordé dans son avis le contexte de son auto-saisine, l'obligation spécifique de déposer une liste des membres d'une association et la problématique générale soulevée par le dépôt de la liste des membres.

La Commission nationale a estimé qu'il était raisonnable de tenir une liste des membres d'une association à des fins de gestion administrative interne et consultable précisément par lesdits membres. Elle s'est par ailleurs interrogée sur la finalité poursuivie par le fait de rendre accessible cette liste à des tiers.

De plus, la Commission nationale a constaté dans son avis qu'il existe actuellement une contradiction entre l'article 10 de loi modifiée du 21 avril 1928 et le respect de la vie privée des membres d'une association, ainsi que la protection de leurs données à caractère personnel au regard du RGPD. Par ailleurs, comme le montre les réclamations et demandes d'informations reçues par la CNPD, les associations se retrouvent momentanément dans une situation juridique incertaine, entre l'obligation de déposer la liste des leurs membres auprès du RCS, résultant d'une loi nationale vieille de 90 ans, d'un côté et le respect des dispositions du RGPD, norme législative supérieure, d'autre côté. Afin de parer à cette insécurité juridique et d'assurer la conformité du cadre légal luxembourgeois au RGPD, la CNPD a donc estimé nécessaire de procéder rapidement à la modification de l'article 10 de la loi modifiée du 21 avril 1928. En effet, la CJUE exige des Etats membres de l'Union européenne de mettre en conformité leurs législations et leurs réglementations nationales existantes avec les règlements européens, en jugeant que *« la primauté et l'effet direct des dispositions du droit communautaire ne dispensent pas les États membres de l'obligation d'éliminer de leur ordre juridique interne les dispositions incompatibles avec le droit communautaire; en effet, leur maintien engendre une situation de fait ambiguë, en laissant les sujets de droit concernés dans un état d'incertitude quant aux possibilités qui leur sont réservées de faire appel au droit communautaire.»*

F) CONTRÔLE DE L'ACQUISITION ET DE LA DÉTENTION D'ARMES

Le 8 juillet 2019, la CNPD a donné son avis sur le projet de loi n°7425 portant : 1° transposition de la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes ; 2° modification du Code pénal, et 3° abrogation de la loi du 20 avril 1881 concernant le transport et le commerce des matières explosives.

Dans son avis, la CNPD a abordé les questions relatives aux aspects de la protection des données à caractère personnel, soulevées par les articles 13 (Fichier des armes et traitement de données à caractère personnel), 14 (Attestation médicale), 15 (Agrément d'armurier et de commerçant d'armes), 17 (Salariés et collaborateurs des armuriers), 19 (Registre d'armes), 22 (Conditions générales concernant l'octroi des autorisations aux particuliers) et 52 (Contrôles effectués par l'Administration des douanes et accises) du projet de loi.

La Commission nationale a noté que certains éléments relatifs au traitement de données n'ont pas (ou pas suffisamment) été précisés dans le projet de loi et a énuméré dans ses développements les éléments manquants concernant les traitements effectués dans le cadre de la tenue du fichier visé à l'article 13, les spécificités relatives au traitement de données relatives aux infractions pénales et à la santé qui doivent être respectés par le responsable du traitement, les clarifications devant être apportées au registre des armes tenus par les armuriers et à l'accès prévu par l'article 52 du projet de loi pour les agents de l'Administration des douanes et accises.

La CNPD a notamment émis les recommandations suivantes :

- concernant la base juridique sur laquelle se fonde le traitement, la Commission nationale a suggéré que le passage suivant « la personne concernée consent au traitement de ses données à caractère personnel » soit supprimé ;
- concernant la détermination des finalités du traitement, la CNPD a estimé que la finalité telle que rédigée dans le projet de loi était formulée de manière trop vague et devait être précisée ;
- concernant les catégories de données à caractère personnel, la CNPD a recommandé d'énumérer quelles données sont collectées et pour quelles finalités,
- concernant les personnes concernées, la Commission nationale a préconisé que le législateur insère des dispositions concernant les catégories de personnes concernées (acquéreur, fournisseur, titulaire d'une autorisation de détention d'armes…) pour les différents traitements susceptibles d'être mis en œuvre dans le cadre du projet de loi ;
- concernant l'accès aux données à caractère personnel, la CNPD a recommandé de préciser qu'au sein du Ministère de la Justice l'accès aux données soit limité aux seuls agents ayant besoin d'en connaître dans le cadre de leur fonction et d'énumérer les autorités administratives susceptibles d'y avoir accès ;
- concernant la traçabilité des accès, la CNPD a recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début la personne ou le service, au sein de chaque administration concernée, qui aurait accès à l'interface informatique mise à disposition par le CTIE, et à quelles données précises cette personne ou ce service aurait accès.

G) MESURES MACROPRUDENTIELLES PORTANT SUR LES CRÉDITS IMMOBILIERS RÉSIDENTIELS

Le 8 août 2019, la CNPD a avisé les amendements gouvernementaux au projet de loi relatif à des mesures macroprudentielles portant sur les crédits immobiliers résidentiels et portant modification de la loi modifiée du 5 avril 1993 relative au secteur financier, et de la loi du 1er avril 2015 portant création d'un comité du risque systémique et modifiant la loi modifiée du 23 décembre 1998 relative au statut monétaire et à la Banque centrale du Luxembourg.

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

Dans son avis du 29 mars 2018 (document parlementaire 7218/06), la Commission nationale avait déjà eu l'occasion de se prononcer au sujet de ce projet de loi et s'était limitée à des remarques relatives à son

article 2, en particulier concernant l'utilisation des termes « informations agrégées », qu'elle recommandait de remplacer par « données agrégées et anonymisées » (s'il s'agit en effet de données anonymes ou rendues anonymes).

H) ANNUAIRES RÉFÉRENTIELS D'IDENTIFICATION DES PATIENTS ET DES PRESTATAIRES

Le 18 octobre 2019, la CNPD a publié un avis complémentaire relatif au projet de règlement grand-ducal précisant les modalités de gestion de l'identification des personnes et les catégories de données contenues dans les annuaires référentiels d'identification des patients et des prestataires.

La CNPD avait déjà rendu, le 21 décembre 2018, un premier avis relatif au projet de règlement grand-ducal précisant les modalités de gestion de l'identification des personnes et les catégories de données contenues dans les annuaires référentiels d'identification des patients et des prestataires dans lequel elle avait souligné l'importance de conférer une base légale au dispositif d'identitovigilance développé par l'Agence eSanté d'une part, et aux annuaires référentiels d'identification des patients et des prestataires de soins de santé, d'autre part, en permettant de garantir les objectifs de sécurité et de qualité de l'information qui sous-tendent la mise en place desdits outils par l'Agence eSanté. Le Conseil d'État s'était déjà prononcé sur le projet de règlement grand-ducal dans un avis rendu le 27 novembre 2018.

La Commission nationale a remarqué dans son avis que certaines de ses observations avaient été prises en compte par les auteurs des amendements. Elle a ainsi limité ses observations aux amendements du projet de règlement grand-ducal pour lesquels les auteurs n'avaient pas suivi les recommandations de la CNPD.

I) MODALITÉS ET CONDITIONS DE MISE EN PLACE DU DOSSIER DE SOINS PARTAGÉ

Le 18 octobre 2019, la CNPD a avisé les amendements au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé.

Pour rappel, la CNPD avait rendu, le 5 avril 2018, un premier avis relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé dans lequel elle a formulé toute une série d'observations sur les dispositions dudit projet ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel.

Le Conseil d'État quant à lui s'était prononcé sur le projet de règlement grand-ducal dans un avis rendu le 23 octobre 2018, dans lequel il a repris de nombreuses critiques émises par la Commission nationale dans son avis précité du 5 avril 2018.

La Commission nationale s'est félicitée du fait que certaines de ses remarques ont été prises en compte par les auteurs des amendements.

Dans son avis 2019, elle a notamment abordé les questions relatives au principe de licéité d'un traitement de données à caractère personnel, à la responsabilité du traitement, aux modalités d'ouverture et de fermeture du DSP, à l'accès au DSP par les professionnels de santé, à la conservation des données et à la sécurité de la plateforme.

J) QUALIFICATION INITIALE ET FORMATION CONTINUE DES CONDUCTEURS DE CERTAINS VÉHICULES ROUTIERS

Le 15 novembre 2019, la CNPD a avisé le projet de loi n°7462 portant modification de la loi modifiée du 5 juin 2009 relative à la qualification initiale et à la formation continue des conducteurs de certains véhicules routiers

affectés aux transports de marchandises ou de voyageurs et modifiant la loi modifiée du 27 juillet 1993 ayant pour objet 1. le développement et la diversification économiques et 2. l'amélioration de la structure générale et de l'équilibre régional de l'économie.

Le projet de loi a pour objet de transposer en droit national la directive (UE) 2018/645 du Parlement européen et du Conseil du 18 avril 2018 modifiant la directive 2003/59/CE relative à la qualification initiale et à la formation continue des conducteurs de certains véhicules routiers affectés aux transports de marchandises ou de voyageurs ainsi que la directive 2006/126/CE relative au permis de conduire. L'une des nouveautés de la directive est la mise en place entre les États-membres d'un réseau électronique dont le but est de permettre l'échange, entre les États-membres, d'informations sur les certificats de formation délivrés ou retirés aux conducteurs de certains véhicules routiers.

Dans son avis, la CNPD s'est limitée à commenter les nouvelles dispositions introduites par la directive concernant la mise en place d'un réseau électronique entre les États-membres, tel que décrit ci-avant. Ces dispositions ont été transposées en droit national à l'article 4 du projet de loi qui insère un nouvel article 6 bis intitulé « Banque de données électronique et échanges de données » dans la loi modifiée du 5 juin 2009.

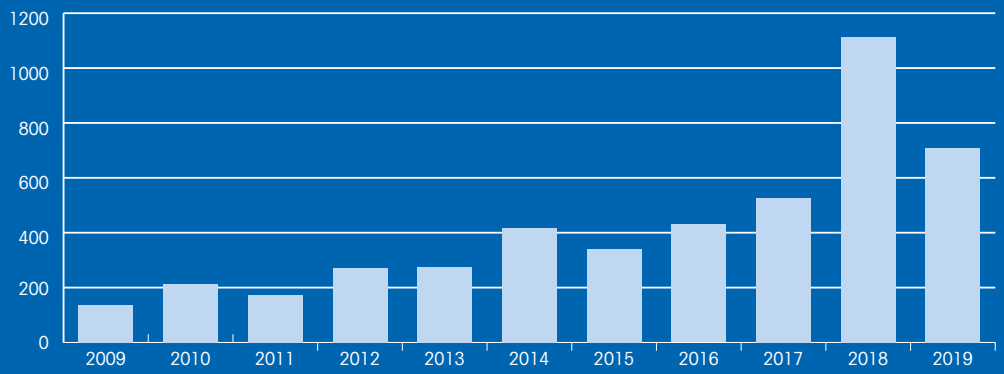
K) AIDE AU FINANCEMENT DES GARANTIES LOCATIVES

Le 25 novembre 2019, la CNPD a donné son avis à l'égard des amendements gouvernementaux au projet de règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14quater-1 et 14quater-2 de la loi modifiée du 25 février 1979 concernant l'aide au logement.

La CNPD a limité ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par les articles 2 et 3 du projet de règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14quater-1 et 14quater-2 de la loi modifiée du 25 février 1979 concernant l'aide au logement. Elle ne s'est pas prononcée au sujet du projet de règlement grand-ducal déterminant les critères minimaux de salubrité, d'hygiène, de sécurité et d'habitabilité auxquels doivent répondre les logements et chambres donnés en location ou mis à disposition à des fins d'habitation.

En date du 14 septembre 2018, la Commission nationale avait émis un avis relatif tant à ce projet de loi, qu'au projet de règlement grand-ducal sous examen (délibération n°450/2018, document parlementaire 7258/03). Dans l'avis de 2019, elle s'est limitée aux changements introduits par les amendements au projet de règlement grand-ducal et a renvoyé pour le surplus à ses commentaires et suggestions émis à l'occasion de son précédent avis.

ÉVOLUTION DU NOMBRE DE DEMANDES DE RENSEIGNEMENT PAR ÉCRIT



1.6 TRAITEMENT DES DEMANDES DE RENSEIGNEMENTS

La Commission nationale a reçu 708 demandes de renseignement par écrit en 2019.

Tout en restant en-dessous du pic de demandes de 2018, le nombre de sollicitations restent élevées. Alors qu'en 2018, avec l'entrée en application du RGPD, un grand nombre de demandes étaient en lien avec des questions plus générales relatives à la mise en conformité à la nouvelle législation, les sollicitations sont devenues plus spécifiques, démontrant une plus grande sensibilisation des acteurs en 2019 au sujet de la protection des données.

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

Les thématiques qui reviennent le plus souvent sont les suivantes :

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

D'autres questions récurrentes concernent notamment :

- le champ d'application territorial du RGPD (pour les sociétés établies en dehors de l'UE, y compris les questions liées à la désignation d'un établissement principal ou unique et d'une autorité de contrôle principale) ;
- le système de certification d'opérations de traitement introduit par le RGPD (Quel est le champ d'application de la certification « GDPR-CARPA » ?) ;

- l'anonymisation et la pseudonymisation des données à caractère personnel (et leur impact concernant les règles applicables en matière de protection des données) ;
- le consentement des personnes concernées (Dans quels cas et sous quelles conditions doit-il être demandé ?) ;
- les cookies (Quelles sont les règles pour les hébergeurs de sites internet utilisant des cookies ?) ;
- les violations de données (Qu'est-ce qui constitue une violation de données et à partir de quel moment faut-il notifier la CNPD ?) ;
- le droit à l'image (pour les ASBL, sur les réseaux sociaux, en milieu scolaire, etc.) ;
- les drones (pour les personnes concernées : un drone a survolé ma propriété, quels sont mes moyens d'actions ? pour les responsables de traitement : dans quelles conditions et où puis-je piloter un drone et filmer à l'aide de celui-ci ?) ;
- les questions liées à l'utilisation du « GDPR Compliance Support Tool » de la CNPD ;
- la durée de conservation des données (Combien de temps avons nous le droit de conserver les données à caractère personnel de nos clients ? ou de nos employés ?) ;
- la prospection / le marketing (Dans quelles conditions pouvons-nous envoyer des newsletters ou mails publicitaires à nos clients ?) ;
- les ressources humaines (Dans quelles conditions un potentiel employeur peut-il se renseigner auprès de l'ancien employeur d'un candidat ?) ;
- la sous-traitance (Quelles sont les conditions liées au recours à un sous-traitant ? Est-ce que la CNPD dispose de modèles de contrats de sous-traitance ?) ;
- l'utilisation du numéro de matricule (Dans quelles conditions pouvons-nous utiliser le numéro de matricules de nos employés ou de nos clients ?) ;
- les dashcams (L'utilisation de dashcams est-elle admise ou interdite au Luxembourg ?).

2 CONFORMITÉ ET CONTRÔLE

2.1 TRAITEMENTS DES RÉCLAMATIONS

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

En 2019, la CNPD a reçu 625 réclamations :

- 381 personnes ont directement fait appel aux services de la CNPD lorsqu'elles ont estimé qu'il y a eu une violation de la loi ou une entrave à l'exercice de leurs droits.

LE SYSTÈME D'INFORMATION DU MARCHÉ INTÉRIEUR (IMI)

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

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

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

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

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

- déterminer quelle est l'autorité de contrôle chef de file dans un litige transfrontalier;
- coopérer pour parvenir à un règlement des litiges transfrontaliers;
- demander et fournir une assistance aux autorités de contrôle d'autres États membres;
- organiser des opérations communes associant les autorités de contrôle de plusieurs États membres;
- consulter le Comité européen de la protection des données pour obtenir un avis ou une décision contraignante.

- En plus des réclamations au niveau national, s'ajoutent à travers le système européen de coopération 244 réclamations où la CNPD a été ou est l'autorité chef de file présumée (IMI - système d'information du marché intérieur).

Par rapport à l'année précédente, il s'agit d'une augmentation de 175 réclamations, soit 39 %.

Plus d'un quart des réclamations (26 %) a été motivé par le non-respect du droit d'accès par les responsables du traitement. Ces derniers ont refusé aux citoyens d'accéder à leurs données, ignoré leurs requêtes ou ne leur ont pas donné assez de renseignements par rapport aux obligations légales à respecter en matière de droit à l'information et d'accès.

Les demandes d'effacement ou de rectification de données constituent 21 % des réclamations reçues en 2019. Il s'agissait, entre autres, de demandes de fermeture de comptes auprès de services en ligne ou de demandes d'effacement de données personnelles (adresses e-mail, évaluations, etc.) accessibles sur des sites Internet.

LES ACTIVITÉS EN 2019

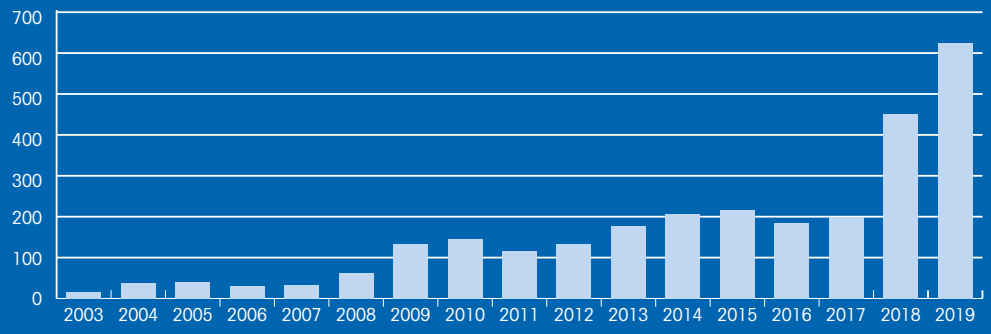
3

11 % des plaintes étaient relatives au droit d'opposition. Celles-ci portent plus particulièrement sur l'exercice du droit d'opposition en matière de prospection. La CNPD a dû intervenir lorsque des liens de désabonnement à prospection dans des courriels n'étaient pas fonctionnels ou lorsque le responsable de traitement ne donnait pas suite aux demandes d'opposition.

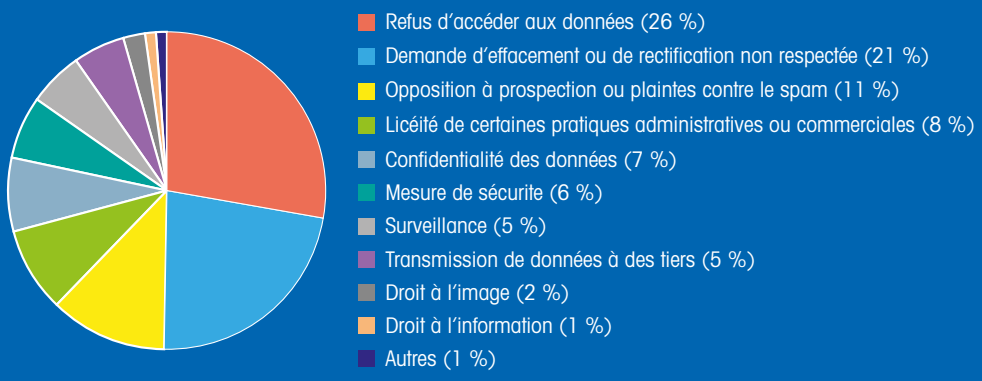
Dans 8% des cas, les réclamants ont demandé à la CNPD de vérifier la licéité de certaines pratiques administratives ou commerciales. Ils ont notamment remis en cause :

- des dispositions relatives à la protection des données mentionnées dans des conditions générales relatives à des commerces ou des services en ligne ;

ÉVOLUTION DU NOMBRE DE RÉCLAMATIONS



MOTIFS DES RÉCLAMATIONS



- la durée de conservation des données collectées ;
- la demande de documents comme la carte d'identité ou le passeport à des fins de vérification d'identité ;
- la publication des données à caractère personnel en ligne (p.ex. sur un réseau social) ;
- la collecte illicite ou excessive de données ;
- la licéité de traitement des dossiers du personnel ;
- la création d'annuaires sans le consentement des personnes concernées ;
- des décisions individuelles automatisées.

La majorité des requêtes liées à la surveillance sur le lieu du travail (5 % des réclamations) concernaient la vidéosurveillance. Des réclamants ont également contacté la CNPD lorsqu'ils ont estimé que des systèmes

de géolocalisation avaient été utilisés par leur employeur de manière illicite (p.ex. surveillance en dehors des heures de travail).

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

2.2 CONTRÔLES EFFECTUÉS

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

- obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel qui sont traitées et à toutes les informations nécessaires à l'exercice de ses missions ;
- obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement ;
- mener des enquêtes sous la forme d'audits sur la protection des données.

La CNPD adopte une approche double en ce qui concerne la vérification de l'application des règles en matière de protection des données. D'un côté, il y a le volet « réactif », largement dirigé par les réclamations, et de l'autre côté le volet « proactif ». La CNPD a le pouvoir de lancer des enquêtes de sa propre initiative. Des contrôles « proactifs » sont effectués auprès d'organisations qui ont été sélectionnées sur base d'un échantillonnage en se basant sur des critères de risque, comme par exemple le secteur d'activité ou la taille. Ces contrôles sont par la suite effectués soit de manière non annoncée (les enquêtes sur place) soit de manière annoncée (les enquêtes sous forme d'audit sur la protection des données).

A) CONTRÔLE SUR PLACE

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

Le nombre d'enquêtes sur place a augmenté de 12 en 2018 à 33 en 2019. Ces enquêtes concernaient notamment les domaines de la vidéosurveillance, de la géolocalisation, de la publicité et du marketing.

B) AUDITS SUR LA PROTECTION DES DONNÉES

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

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

LES ACTIVITÉS EN 2019

3

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

La première moitié de 2019 a été consacrée à la collecte d'information : une trentaine d'entretiens sur place a été conduite. La seconde moitié de l'année a été consacrée à l'analyse des constats pour une prise de position de la part des enquêteurs et des chefs d'enquête.

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

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

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

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

Parallèlement à la campagne DPO, 9 audits réactifs ont été ouverts. Il s'agit de plaintes nationales ou issues du mécanisme de coopération européenne pour lesquelles la CNPD a décidé d'ouvrir un audit. Ces plaintes concernent des problématiques variées : le droit d'accès, la sécurité des données, le processus de recrutement ou encore la gestion des cookies, par exemple.

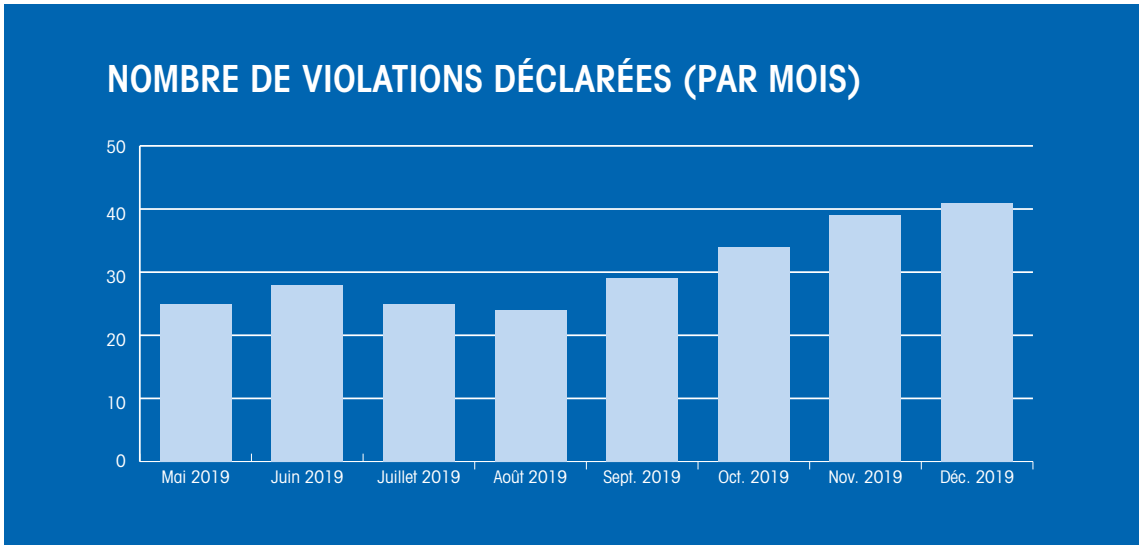
2.3 NOTIFICATION DES VIOLATIONS DE DONNÉES

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

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

A) VIOLATIONS DE DONNÉES DANS LE CADRE DU RGPD

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



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

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

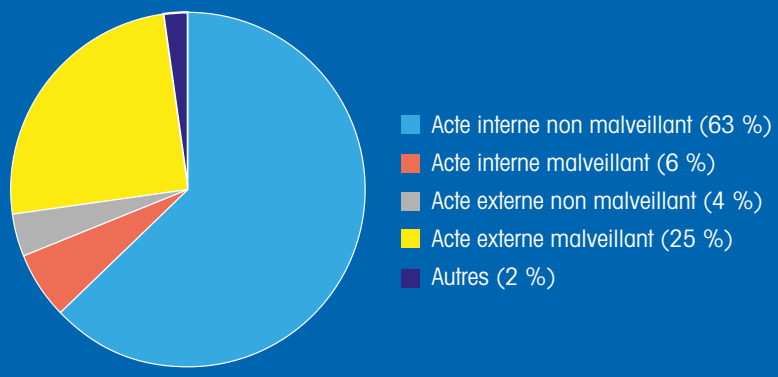
En 2019, 354 violations de données ont été notifiées à la CNPD.

Au total, depuis l'entrée en application du RGPD le 25 mai 2018, la CNPD a reçu 526 violations de données. Cela correspond à presque 28 notifications de violations de données par mois.

LES ACTIVITÉS EN 2019

3

CAUSES DES VIOLATIONS

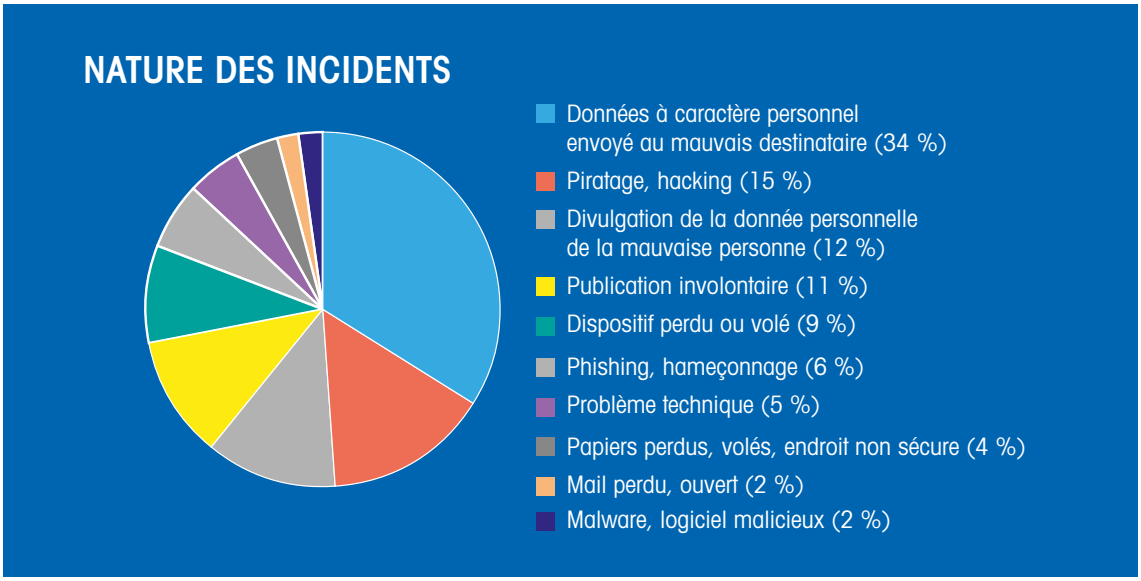


La principale cause de violation de données à caractère personnel reste l'erreur humaine (acte interne non malveillant).

La plupart des erreurs humaines se produisent :

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

Des actes externes malveillants sont à l'origine de plus du quart des violations notifiées. Ce type d'incidents a souvent un impact plus important sur les personnes concernées. Dans de nombreux cas, ces actes ciblent



l'accès ou l'obtention de données qui permettent de réaliser des transactions financières à l'insu des personnes concernées (ex : interception de données de cartes de paiement bancaire, phishing pour obtenir les informations de connexions à un service de paiement, usurpation d'identité pour effectuer une transaction financière, etc.).

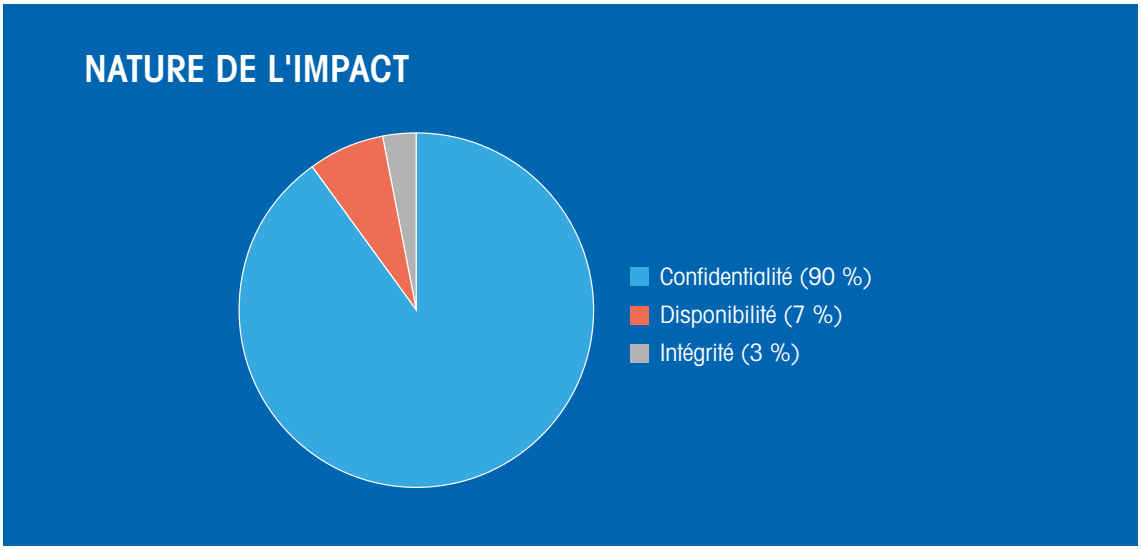
Les actes internes malveillants se sont produits principalement lors de départs, volontaires ou non, d'employés d'une organisation: cette situation amène des personnes à copier des données pour potentiellement les utiliser dans leur nouvelle situation.

De même, les situations de cessation d'activité / fusion / rachat de sociétés sont des périodes à risque pour des exfiltrations non autorisées de données.

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

LES ACTIVITÉS EN 2019

3

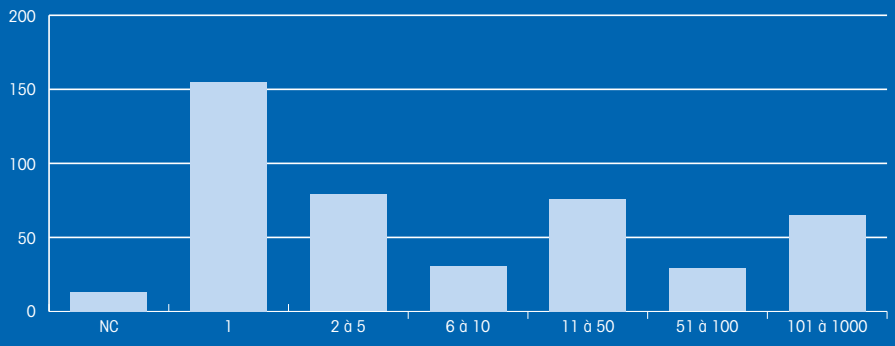


La quasi-totalité des violations de données ont un impact en rapport avec la perte de confidentialité des données concernées.

Plus de la moitié des incidents de sécurité est détectée au plus tard 5 jours après leur survenance. Toutefois, la CNPD a constaté que presque 10% des violations de données à caractère personnel ne sont détectés qu'au minimum un mois après s'être produits : il s'agit plus particulièrement d'incidents liés à des violations continues de la politique de sécurité de l'organisation (p.ex. : le personnel de direction envoie les données professionnelles sur leur email personnel pour travailler du domicile et l'email personnel est piraté), de données utilisées par des employés lors d'un départ d'une organisation et également de vol de données liée à des piratages non détectés.

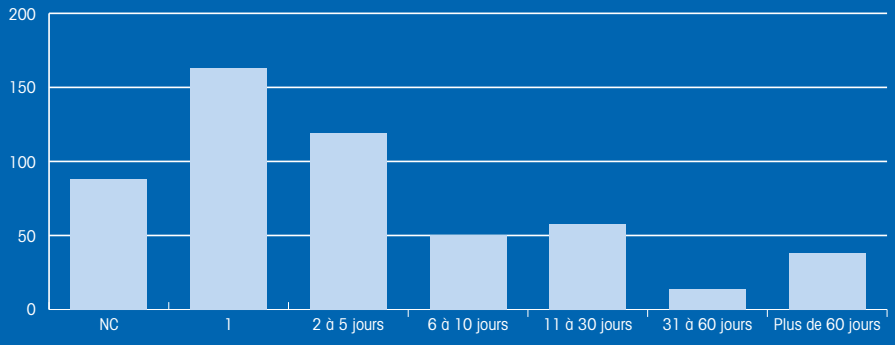
La CNPD attire également l'attention des responsables du traitement sur le fait qu'un certain nombre d'actes de piratage et de phishing sont ciblés sur le personnel de la direction d'une organisation et leur entourage (ex : assistant / secrétariat de la direction). Ces actes malveillants ont souvent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

NOMBRE DE PERSONNES POTENTIELLEMENT IMPACTÉES PAR INCIDENT



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

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



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

Points d'attention identifiés :

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

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

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

B) VIOLATIONS DE DONNÉES DANS LE SECTEUR DES COMMUNICATIONS ÉLECTRONIQUES

Conformément au règlement (UE) No. 611/2013 de la Commission européenne du 24 juin 2013, les fournisseurs de services de communications électroniques accessibles au public, tels que les entreprises de téléphonie fixe/mobile ou les fournisseurs d'accès à Internet, doivent avertir la CNPD endéans les 24 heures suivant le constat d'une violation de sécurité et de confidentialité des données à caractère personnel et, de surcroît, informer leurs abonnés au cas où l'incident constaté est susceptible d'affecter défavorablement le niveau de protection de leur vie privée et des données les concernant.

Afin de faciliter la tâche aux fournisseurs de services de communications électroniques, la Commission nationale propose un formulaire de notification d'une violation de sécurité disponible sur son site Internet. Ce formulaire reprend toutes les questions pertinentes auxquelles les fournisseurs devront répondre dans une telle situation.

En 2019, aucune violation de données dans le secteur des communications électroniques n'a été signalée à la CNPD.

2.4 DÉSIGNATION DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES

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

En 2019, 272 responsables du traitement ont communiqué les coordonnées de leur DPD à la CNPD. Depuis le 25 mai 2018, 1090 responsables du traitement ont effectué cette démarche.

Au total, 731 personnes physiques ou morales ont été déclarées auprès de la CNPD, dont 238 en 2019.

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

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

- le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;
- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.

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

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

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

L'analyse d'impact relative à la protection des données permet :

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

L'enjeu est d'apprécier et de gérer les risques pour les droits et libertés des personnes concernées pour construire des traitements conformes au RGPD et respectueux de la vie privée.

LES ACTIVITÉS EN 2019

3

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

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

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

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

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

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

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

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

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

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

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

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

En 2019, la CNPD n'a pas reçu de demande de consultation préalable respectant les critères tels que stipulés dans le RGPD.

2.6 CERTIFICATIONS

La CNPD a continué ses travaux démarrés l'année précédente pour proposer, mettre en place et gérer les activités de certification liées à l'utilisation des instruments de conformité volontaire tels que proposés dans le RGPD. Ces instruments sont voués à permettre aux responsables de traitement de démontrer que leurs opérations de traitement respectent le règlement.

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

Ainsi la CNPD a continué ses travaux, en collaboration avec les entreprises d'audit, sur le développement d'un référentiel de certification basé sur le cadre d'évaluation international de conformité ISAE (« International Standard

on Assurance Engagements »). Elle a également contribué en tant que lead-rapporteur, au Comité Européen pour la Protection des Données, à la mise en place de procédures pour l'adoption des critères d'agrément des organismes de certification, l'adoption des critères de certification et l'adoption d'un label européen pour la certification.

2.7 TRANSFERTS INTERNATIONAUX DE DONNÉES PERSONNELLES

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

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

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

Tout responsable de traitement qui souhaite exporter des données à caractère personnel hors de l'Espace économique européen doit d'abord se renseigner sur le niveau de protection adéquat du pays destinataire. En effet, lorsque le pays tiers est formellement considéré comme offrant un niveau de protection adéquat par la Commission européenne (exemples : la Suisse, le Japon, l'Argentine, le Canada dans certains cas, ou les États-Unis d'Amérique dans certains cas (voir ci-dessous)), le transfert peut être effectué comme s'il s'agissait d'un transfert au sein de l'Espace économique européen.

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

Sur base de la décision d'exécution de la Commission européenne (UE) 2016/1250, certaines entreprises établies dans l'Espace économique européen transféraient les données personnelles qu'elles traitaient à destination des sociétés américaines figurant sur la liste « EU-U.S. Privacy Shield Framework », de la même manière que s'opèrent les transferts vers les pays reconnus comme « adéquats » par la Commission européenne.

Comme indiqué dans l'avant-propos, cette décision d'exécution a été invalidée en juillet 2020 par la Cour de justice de l'Union européenne (CJUE) dans l'affaire Data Protection Commissioner contre *Facebook Ireland et Maximillian Schrems* (Schrems II). Dans son arrêt, la Cour a constaté que le « Privacy Shield » n'assurait pas un niveau de

protection essentiellement équivalent à celui garanti par le RGPD et la Charte des droits fondamentaux de l'UE. Par conséquent, ces entreprises ne peuvent donc plus légitimer leurs transferts vers les États-Unis d'Amérique sur le « EU-U.S. Privacy Shield Framework », mais devront réaliser la même analyse que pour tout autre pays en dehors de l'Espace économique européen ne disposant pas d'un niveau de protection adéquat (voir point b ci-dessous).

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

Pour les pays non membres de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande) qui n'ont pas été reconnus comme offrant un niveau de protection adéquat en matière de protection des données par la Commission européenne, il existe différentes possibilités pour un transfert de données.

Dans un tel cas, la CNPD recommande d'adopter, tout comme ses homologues européens, une approche par étapes fondée sur les meilleures pratiques et consistant à envisager de fournir des garanties adéquates. Les exportateurs de données devraient donc d'abord s'efforcer de trouver des possibilités de procéder au transfert à l'aide de garanties appropriées (clauses contractuelles, règles d'entreprise contraignantes (BCR), codes de conduite, mécanismes de certification ou garanties spécifiques pour le transfert entre autorités ou organismes publics), au besoin en ayant recours à des garanties supplémentaires afin de se conformer à l'arrêt « Schrems II » de la Cour de Justice de l'Union européenne (voir avant-propos et point A ci-dessus), et ne recourir à des dérogations qu'en l'absence de telles garanties.

Les règles d'entreprise contraignantes

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

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

En 2019, la Commission nationale a traité des dossiers concernant des règles d'entreprise contraignantes, dont six en qualité d'autorité principale (c'est-à-dire pour des entreprises multinationales dont l'établissement principal dans l'Union européenne est situé à Luxembourg), deux en qualité d'autorité secondaire (c'est-à-dire en appui de l'autorité de contrôle principale) et 24 en qualité d'autorité concernée.

C) DÉCISION D'ADÉQUATION AVEC LA JAPON

La CNPD contribue aux activités du Comité européen de la protection des données (EDPB). A cet égard, elle a été impliquée dans l'évaluation de la décision d'adéquation avec le Japon de la Commission européenne. Pendant plusieurs mois, elle a examiné le travail réalisé par cette dernière et apprécié l'impact de la libre circulation des données à caractère personnel entre l'Union européenne et le Japon sur les garanties et le degré de protection conférés par les deux économies aux citoyens européens. Le 5 décembre 2018, l'EDPB a adopté son opinion sur la décision d'adéquation révélant l'importance de cette décision d'adéquation puisqu'elle est la première rendue sous l'égide du RGPD.

Pour rappel, la décision d'adéquation avec le Japon a pour objet d'établir un ensemble de règles qui permettent de réduire certaines différences entre les deux systèmes de protection des données et des garanties lors de l'accès aux données des citoyens européens par les autorités publiques japonaises dans le cadre de procédures pénale et de sécurité nationale du pays, ainsi qu'un mécanisme de traitement des plaintes des citoyens européens concernant l'accès à leurs données par les autorités publiques japonaises.

La décision d'adéquation a été adoptée par le Parlement européen le 13 décembre 2018 et par la Commission européenne le 23 janvier 2019.

2.8 MESURES CORRECTRICES ET SANCTIONS

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

Les violations par le responsable du traitement du RGPD peuvent faire l'objet d'amendes pouvant s'élever jusqu'à vingt millions d'euros ou jusqu'à 4% du chiffre d'affaire annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Le RGPD exige que les sanctions soient « effectives, proportionnées et dissuasives » - ceci implique que la taille de l'entreprise, la gravité des faits, l'ampleur de la violation, des dommages, du nombre de personnes touchées, ainsi que le niveau de risque et les moyens d'une entreprise pour se mettre en conformité soient pris en compte.

Entre le 25 mai 2018 et le 31 décembre 2019, 140 réclamations nationales ont conduit à l'adoption de mesures correctrices. Il s'agit des cas où la CNPD a ordonné au responsable du traitement de mettre en place des mesures pour se conformer au RGPD (ex. faire droit à une demande d'accès, d'effacement, d'opposition, modification des notices d'informations afin de se conformer aux exigences des articles 13 et 14 du RGPD, mise en place de mesures de sécurité supplémentaires, etc.). En plus des réclamations introduites au niveau national, s'ajoutent

à travers le système européen de coopération encore 161 réclamations qui ont été clôturées par des mesures correctrices.

La CNPD estime qu'une amende administrative ne peut être prononcée que par la Commission nationale siégeant en formation restreinte de décision sur l'issue de l'enquête conformément à l'article 41 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

En effet, en fonction de la pertinence d'un dossier, la CNPD peut ouvrir une enquête conformément à l'article 37 de la loi du 1er août 2018 précitée. Cela implique une procédure avec deux processus consécutifs (le processus d'enquête mené par un des commissaires en tant que chef d'enquête et un processus de décision par la Commission nationale siégeant en formation restreinte c'est-à-dire composé des trois autres commissaires).

Aucun dossier d'enquête examiné par la formation restreinte en 2019 n'a présenté des violations dont la gravité aurait justifié le prononcé d'une amende administrative. Par conséquent, aucune amende administrative n'a été imposée par la CNPD depuis l'entrée en vigueur de la loi du 1er août 2018.

Or, les enquêtes d'envergure et celles exigeant une collaboration avec une ou plusieurs autorités de surveillance d'autres pays nécessitent des évaluations complexes à la fois juridiques et techniques qui, évidemment, prennent plus de temps pour être conclues.

Fin 2019 plusieurs dossiers d'enquête de ce type ont été en procédure d'examen et seront transférés au collège des commissaires siégeant en formation restreinte pour prise de décisions selon le règlement d'ordre intérieur et le règlement d'enquête en vigueur.

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

La loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données a abrogé la loi modifiée du 2 août 2002, ce qui a également entraîné la suppression de l'autorité de contrôle « Article 17 ». Avec l'entrée en vigueur de la nouvelle loi, les compétences et missions de l'ancienne autorité de contrôle « Article 17 » ont été conférées à la CNPD avec effet au 20 août 2018. La présente section du rapport d'activité de la CNPD couvre dès lors la période allant du 20 août 2018 au 31 décembre 2019.

La CNPD est donc aussi devenue 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

LES ACTIVITÉS EN 2019

3

l'État, l'Autorité nationale de sécurité, l'Administration des Douanes, etc. 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.

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.

A) DEMANDES D'INFORMATION

La CNPD a traité 56 demandes de renseignements écrites et orales en matière de traitement de données dans le domaine répressif.

Suite aux débats publics autour du « Fichier central » opéré par la Police grand-ducale, de nombreux citoyens ont voulu exercer leur droit d'accès et ont saisi la CNPD pour savoir si la Police traitait des données les concernant dans ce fichier. Or, comme le droit d'accès aux données ne peut pas être exercé auprès de la CNPD, mais doit s'exercer directement auprès du responsable du traitement, la CNPD a traité au cours de l'été/automne 2019 34 demandes à ce sujet et a invité les citoyens à formuler leurs demandes d'accès directement auprès de la Police. Elle a par ailleurs publié une guidance à ce sujet sur son site internet pour informer et orienter les citoyens. D'autres demandes de ce genre concernaient aussi d'autres autorités comme p.ex. l'Administration des Douanes et accises ou le Service de renseignement de l'État.

Sans prétendre à l'exhaustivité, la CNPD a également été sollicitée pour répondre à des questions en matière pénale ou de sécurité publique comme p.ex. autour des thématiques suivantes :

- Interprétation 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,* notamment de son champ d'application, de la définition des autorités répressives et l'interaction avec les dispositions du RGPD ;
- Vidéosurveillance dans les lieux publics et dans les lieux privés ;
- Transmission de données à caractère personnel par des entités privées à des autorités répressives nationales et étrangères.

B) AVIS

La CNPD a adopté 5 avis relatifs aux traitements de données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

Fichier central de la Police grand-ducale au regard de la législation sur la protection des données
Le 13 septembre 2019, la CNPD a adopté un avis sur le fichier central de la Police grand-ducale.

Eu égard à la mission de conseil qui lui est attribuée, la CNPD a été sollicitée par Monsieur le Ministre de la Sécurité intérieure pour rendre un avis au sujet du fichier central de la Police grand-ducale au regard de la législation en matière de protection des données.

Si le domaine des fichiers de la Police est peu connu et suscite de réelles inquiétudes des citoyens quant au respect des libertés publiques et de la protection de leurs données personnelles, les fichiers constituent néanmoins des outils indispensables à l'exécution des missions des forces de police.

Afin de répondre au mieux à la demande d'avis qui lui a été soumise, la CNPD a pris en compte les préoccupations citoyennes, les nombreuses questions parlementaires émanant des députés et les réponses à ces interrogations par les ministres concernés. La CNPD a également sollicité les autorités de la protection des données d'autres Etats membres afin que ces dernières la renseignent quant au cadre légal en matière de protection des données encadrant les fichiers policiers dans leurs pays. En guise de préparation de son avis, la CNPD s'est réunie à plusieurs reprises avec la Police grand-ducale, l'Inspection générale de la police et le Ministère de la sécurité intérieure, dans le but d'approfondir sa compréhension de la gestion et de l'exploitation qui est faite du fichier central.

La première partie de l'avis est consacrée à l'encadrement légal du fichier central conféré 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 intérieure. Les principes applicables au traitement des données à caractère personnel effectué via le fichier central y sont analysés ainsi que les droits des personnes concernées par le traitement de leurs données à travers le fichier central, puis les obligations du responsable du traitement quant à la gestion et l'exploitation dudit fichier. Une deuxième partie de l'avis, porte sur la qualité du cadre légal encadrant le fichier central. La qualité est évaluée au regard du respect des principes généraux relatifs au traitement des données à caractère personnel en matière pénale puis au regard du cadre légal d'autres États-Membres à savoir la France, la Belgique et l'Allemagne.

Dans sa conclusion, la CNPD considère qu'une amélioration de la loi encadrant la matière est opportune. Elle propose donc au législateur de préciser la législation nationale à cet égard en vertu de l'article 1.3 de la Directive dite « police-justice » et à la lumière de la jurisprudence des Hautes juridictions européennes. En outre, la CNPD suggère que la loi sur la Police devrait être complétée de dispositions précisant le principe et les finalités spécifiques des fichiers opérés par la Police grand-ducale pour les besoins d'exécution de ses missions, les délais de conservation des données ou les critères applicables pour déterminer les durées de conservations des données, ainsi que les autres aspects essentiels des traitements de données opérés par la Police grand-ducale. In fine, elle affirme que les mesures législatives à adopter devraient préciser le cadre législatif général posé par la loi de transposition quant aux aspects essentiels des traitements de données, mais aussi prévoir la possibilité d'adopter des règlements grand-ducaux pour régler les modalités moins essentielles, à la lumière de la jurisprudence de la Cour Constitutionnelle.

Vidéosurveillance des espaces et lieux publics à des fins de sécurité publique

Eu égard à la mission de conseil qui lui est attribuée, mais également de la tendance générale du renforcement de la surveillance des citoyens afin de pallier à l'insécurité et face aux préoccupations du public à ce sujet, la Commission nationale a rendu un avis circonstancié en date du 15 mars 2019 sur la création et l'exploitation

par la Police grand-ducale d'un système de vidéosurveillance policière (ci-après désigné « VISUPOL ») au sein de zones de sécurités ciblées à Luxembourg-ville.

L'auto-saisine de la CNPD est intervenue dans le cadre de l'abrogation de la base légale de VISUPOL suite à l'entrée en application de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Les récentes modifications du cadre légal étant rappelées, la CNPD a adopté une approche globale quant à l'utilisation de dispositifs de vidéosurveillance à des fins policières à savoir, la prévention, la recherche et la constatation des infractions. Dans son avis, elle est ainsi revenue sur les caractéristiques et les enjeux de la vidéosurveillance à des fins policières dans l'espace public (I), réflexion qui a pour objet de mettre en exergue l'importance de l'encadrement légal de la surveillance et du contrôle de l'espace public (II).

Selon la CNPD, l'étude des caractéristiques et des enjeux de la vidéosurveillance à des fins policières dans l'espace public, la surveillance, le contrôle social qui en émanent et l'impact de tels dispositifs dans les droits fondamentaux et les libertés reconnues aux individus, sont autant de raisons qui justifient l'importance de l'encadrement légal des dispositifs tels que VISUPOL.

En effet, la CNPD a constaté que comme tout dispositif de vidéosurveillance, VISUPOL est un instrument qui génère une surveillance permanente et un contrôle des individus. Par conséquent, ce dispositif de surveillance policière effectue une ingérence dans le droit à la vie privée et à la protection des données. Il est également susceptible d'entraver le droit à la non-discrimination et de limiter la libre circulation des personnes au sein de l'espace public. Néanmoins, la Commission nationale a rappelé que de telles limitations sont possibles à condition d'être légalement prévues. L'existence d'un tel impératif s'explique notamment par le fait que les personnes dont les droits fondamentaux et les libertés sont limités doivent disposer de garanties suffisantes permettant de se protéger efficacement contre les risques d'abus à leur encontre.

La base légale est également utile aux législateurs et aux juges dans l'appréciation de la nécessité et du caractère proportionné de la mesure qui sont des conditions parmi d'autres que les ingérences doivent remplir. Par conséquent, elle permet de s'assurer que l'installation et l'utilisation de la vidéosurveillance à des fins policières répond à des critères objectifs tel que la lutte contre la délinquance et non subjectifs tel que le sentiment d'insécurité ressenti par les individus.

Ainsi, compte tenu de l'abrogation de la loi de 2002 et des règlements grand-ducaux sur lesquels le dispositif VISUPOL repose et les termes généraux dont fait preuve la loi relative aux missions de la Police grand-ducale, la CNPD a suggéré dans son avis que les dispositions légales de cette dernière soient davantage précisées afin d'inclure VISUPOL dans son champ d'application.

Toutefois, la CNPD s'est demandée s'il ne serait pas plus opportun que le Luxembourg se dote d'une loi spécifique encadrant l'installation et l'exploitation de dispositif de vidéosurveillance dans l'espace public à des fins policières comme le font la France, la Belgique et l'Allemagne.

La CNPD a précisé que son avis n'est pas limité au dispositif VISUPOL de la Police grand-ducale qui, pour l'instant, n'est opérée que sur le seul territoire de la Ville de Luxembourg. En effet, dans la mesure où les responsables de certaines communes ont aussi manifesté leur intention de vouloir surveiller des espaces et lieux publics situés sur leurs territoires communaux, l'avis a une portée générale qui a vocation à couvrir tout dispositif de vidéosurveillance, ayant une finalité de sécurité publique, peu importe qu'il soit opéré au niveau national par la Police grand-ducale ou au niveau local par des communes.

Ainsi, quel que soit le choix de base légale, celle-ci aura pour effet de mettre en exergue qu'au sein d'une démocratie telle que le Luxembourg, un des pays fondateurs de l'Union européenne et protecteurs de ses valeurs, la Police grand-ducale ou encore les communes, exercent leurs missions de surveillance résultant d'une interaction complexe entre des règles juridiques, organisationnelles, professionnelles, situationnelles et interactionnelles.

Recours à la vidéosurveillance par les communes
Le 10 mai 2019, la CNPD a rendu un avis circonstancié relatif au recours à la vidéosurveillance par les communes. Suite à l'entrée en vigueur de la nouvelle législation en matière de protection des données, la CNPD a publié au mois d'août 2018 des lignes directrices en matière de vidéosurveillance. Sans vouloir prétendre à l'exhaustivité, la CNPD y a rappelé certains principes et certaines obligations applicables en matière de vidéosurveillance. Par conséquent, la CNPD conseille dans son avis aux communes de se référer à ces lignes directrices afin d'avoir un aperçu des règles applicables en la matière.

Afin de bien saisir les enjeux que soulèvent l'installation et l'exploitation des dispositifs de vidéosurveillance au sein des communes et les problématiques qui en émanent, la CNPD a fait une distinction dans son avis entre les lieux surveillés d'une part, et les finalités poursuivies par le responsable de traitement lors du recours auxdits dispositifs d'autre part. Ces enjeux et problématiques ont été mis en lumière à travers trois exemples dans son avis.

En conclusion, la CNPD a réitéré sa recommandation au gouvernement d'introduire un cadre législatif spécifique en la matière, lequel pourrait intégrer et clarifier les interactions et les compétences respectives des bourgmestres et de la Police grand-ducale.

Autorité nationale de sécurité
Le 17 décembre 2019, la CNPD a avisé le projet de loi n°6961 portant 1. création de l'Autorité nationale de sécurité (ci-après : « ANS ») et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2) du Code pénal.

Entre 2013 et 2018 la CNPD avait déjà avisé des projets de loi et projets de règlements grand-ducaux en relation avec la thématique.

Dans l'avis de 2019, la CNPD a notamment abordé les points suivants : l'accès direct de l'ANS, par un système informatique, à la partie « recherche » de la banque de données nominatives de police général, la compétence de la CNPD de surveiller l'accès prévu par le paragraphe (1) de l'article 28 de la loi modifiée du 15 juin 2004, la durée de conservation des données relatives à l'enquête de sécurité ainsi que les critères d'appréciation que l'ANS prend en compte en matière de garanties de discrétion, loyauté, fiabilité et intégrité.

Police et exploitation de l'aéroport de Luxembourg
Le 17 décembre 2019, la CNPD a adopté son avis sur le projet de loi n°7475 portant modification de la loi modifiée du 26 juillet 2002 sur la police et sur l'exploitation de l'aéroport de Luxembourg ainsi que sur la construction d'une nouvelle aérogare ; 2. au projet de règlement grand-ducal relatif à la sûreté de l'aviation civile et aux conditions d'accès à l'aéroport de Luxembourg.

C) RÉCLAMATIONS

La CNPD a été saisie de 10 réclamations en matière pénale et de sécurité nationale dans des cas où les responsables de traitement n'ont pas fait droit, n'ont pas répondu du tout ou ont répondu de manière insuffisante à des demandes d'accès aux données de citoyens.

D) NOTIFICATION DES VIOLATIONS DE DONNÉES

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

Entre le 20 août 2018 (entrée en vigueur de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données) et le 31 décembre 2019, la CNPD a reçu deux notifications de violations de données concernant des traitements de données à caractère personnel en matière pénale, ainsi qu'en matière de sécurité nationale.

E) CONTRÔLES PRÉVUS PAR DES DISPOSITIONS LÉGALES SPÉCIFIQUES

En matière pénale et de la sécurité nationale, certaines dispositions législatives nationales et européennes prévoient que la CNPD effectue des contrôles/audits spécifiques et réguliers :

- Au niveau de textes nationaux :
- Loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière ;
- Loi du 18 juillet 2018 sur la Police grand-ducale ;
- Loi du 18 juillet 2018 sur l'Inspection générale de la Police ;

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

- Au niveau de textes européens :
La CNPD doit par ailleurs procéder tous les quatre ans à des audits de protection des données au niveau des parties nationales des systèmes d'information européens SIS II et VIS ainsi qu'à des revues régulières des logs de ces systèmes d'informations, sur base des textes législatifs européens suivants :

- RÈGLEMENT (CE) No 767/2008 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États-membres sur les visas de court séjour (règlement VIS) ;
- DÉCISION 2007/533/JAI DU CONSEIL du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

F) RÉUNIONS

La CNPD a eu une réunion avec la Police grand-ducale concernant l'implémentation de la « loi du 1er août 2018 relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave ».

Elle a participé à deux réunions interministérielles dans le cadre du groupe de travail SIS recast/Interopérabilité focalisant sur l'analyse de trois règlements UE 2018/1860 – 2018/1861 – 2018/1862 concernant l'utilisation du système d'information Schengen (SIS), ainsi que sur deux règlements UE 2019/817 – 2019/818 concernant l'interopérabilité.

Ont également eu lieu plusieurs réunions entre le Service de renseignement de l'État et la CNPD.

Enfin, dans le contexte de son avis sur le « Fichier central » de la Police grand-ducale, la CNPD s'est réunie à plusieurs reprises avec la Police grand-ducale, l'Inspection générale de la police et le Ministère de la sécurité intérieure.

G) COOPÉRATION EUROPÉENNE

Coopération au niveau de l'EDPB
La CNPD a pris part aux travaux du Comité européen de la protection des données (CEPD ou « EDPB » en anglais) en matière pénale ainsi qu'en matière de sécurité nationales. Parmi les sujets traités étaient :

- La préparation du Brexit dont l'impact sur les frontières, la libre circulation et l'échanges des données entre les forces de l'ordre des Etats-membres et du Royaume-Uni, dont notamment les données PNR dites « données passagers » transmises par les transporteurs aériens européens aux forces de l'ordre du Royaume-Uni en cas de la sortie de ce dernier de l'Union européenne.
- L'affaire Schrems II : la Cour de Justice de l'Union européenne (ci-après désignée CJUE) a souhaité entendre la Présidente de l'EDPB afin de l'éclairer quant au degré de protection des données assuré par les États-Unis.

Coopération avec le Contrôleur européen de la protection des données (EDPS)
La législation européenne prévoit que les autorités de contrôle des États-membres contrôlent et supervisent ensemble avec le Contrôleur européen de la protection des données (EDPS), les systèmes d'information européens, à savoir le Système d'Information Schengen II (SISII), le système d'information Europol ainsi que le système d'information des Douanes, opérés par les autorités répressives compétentes.

Dans ce contexte, la CNPD a participé aux réunions bi-annuelles des autorités de contrôle communes suivantes :

- Groupe de coordination du contrôle du SIS II
- Comité de coopération Europol
- Groupe de coordination du contrôle du système d'information européen des Douanes

2.10 RÉTENTION DE DONNÉES DE TRAFIC ET DE LOCALISATION

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

Or, la directive a été annulée par la Cour de justice de l'Union européenne en date du 8 avril 2014 par l'arrêt « Digital Rights Ireland ». Les lois de transposition nationales n'ont toutefois pas été modifiées en conséquence

et la Commission nationale n'a pas reçu d'instruction dans ce cadre par son Ministère de tutelle. Elle continue à lui transmettre annuellement en vue de leur continuation à la Commission européenne des statistiques sur la conservation des données au titre des articles 5 et 9. A cet effet, les fournisseurs de services ou opérateurs conservent et continuent à la Commission nationale, sur demande de celle-ci, les informations comprenant notamment :

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

En 2019, les autorités compétentes ont fait 2 601 demandes auprès des opérateurs. Ce chiffre a baissé par rapport à l'année 2018 où 4 766 demandes avaient été faites. Sur les 2 601 demandes, 493 demandes n'ont pas pu être satisfaites.

3 TRAVAIL AU NIVEAU INTERNATIONAL

L'activité de la Commission nationale a également été marquée par une forte participation aux travaux européens, dominés par des dossiers complexes et techniques. Cet engagement a été nécessaire pour appréhender la matière dans toute son envergure et sa complexité.

La Commission nationale, représentée par un ou plusieurs de ses membres, a participé en 2019 à différents groupes de travail 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 européennes ainsi que le Contrôleur européen à la protection des données (CEPD) ;
- du « Groupe de Berlin », dédié à la protection des données dans le secteur des communications électroniques ;
- de la conférence des commissaires européens à la protection des données à Tbilisi ;
- de la conférence internationale des commissaires à la protection des données et de la vie privée à Tirana ;
- du séminaire européen « Case Handling Workshop » à Bruxelles.

3.1 LE COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES

Le Comité Européen de la Protection des Données (EDPB – European Data Protection Board) est un organe européen indépendant qui contribue à l'application cohérente des règles en matière de protection des données

au sein de l'Union européenne et encourage la coopération entre autorités de l'UE chargées de la protection des données.

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

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

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

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

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

Lors de 11 réunions plénières en 2019, l'EDPB a adopté de nombreux documents de travail, guidances et lettres. Ces documents sont résumés ci-dessous et peuvent être téléchargés dans leur version complète sur Internet[5].

A) PARTICIPATION AUX SOUS-GROUPES (« EXPERT SUBGROUPS »)

A côté des réunions plénières, les autorités de protection des données de l'Union européenne se réunissent au sein de sous-groupes thématiques (juridiques et informatiques). De nombreuses discussion ont lieu dans les sous-groupes afin de trouver un consensus ou une majorité. Les prises de décisions ont lieu lors des plénières mensuelles ou par procédure écrite.

En 2019, la CNPD a participé à 90 réunions des sous-groupes (« Expert SubGroups ») suivants :

- Border, Travel and Law Enforcement
- Compliance, e-Government and Health
- Cooperation
- Enforcement

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

- Financial Matters
- Fining Taskforce
- International Transfer
- IT User
- Key Provisions
- Strategic Advisory
- Social Media
- Technology

Dans ce cadre, la CNPD envoie des représentants aux réunions à Bruxelles ou, lorsque cela n'est exceptionnellement pas possible, participe à ces réunions par téléconférence.

L'autorité de protection des données luxembourgeoise a par ailleurs pris un rôle plus actif comme rapporteur pour les sujets suivants :

- The internal guidance to set up working procedures for delivering consistent opinions under national certification schemes ;
- The internal guidance on procedures for EDPB approval of criteria leading to the European Data Protection Seal.

De plus, la CNPD a été co-rapporteur pour les thématiques suivantes :

- Guidelines on PSD2 and the GDPR ;
- Guidelines on blockchain ;
- Use and retention of credit cards data ;
- Guidelines on connected assistants ;
- Opinion on the COM proposal for an e-evidence regulation ;
- Opinion on the Japan Adequacy Decision ;
- Guidelines on data subject rights.

B) DOCUMENTS ADOPTÉS EN 2019

En 2019, l'EDPB a notamment adopté les documents suivants :

Lignes directrices 1/2019 sur les codes de conduite et les organismes de contrôle en vertu du RGPD
L'objectif de ces lignes directrices est de fournir des conseils pratiques et une assistance dans l'interprétation des articles 40 et 41 du RGPD. Elles visent à clarifier les procédures et les règles relatives à la soumission, à l'approbation et à la publication des codes au niveau national et international. Elles définissent par ailleurs

les critères minimaux requis par une autorité de contrôle avant d'accepter de procéder à un examen et à une évaluation approfondie d'un code. En outre, elles déterminent les facteurs relatifs au contenu à prendre en compte lors de l'évaluation de la capacité d'un code particulier à fournir et à contribuer à l'application effective du RGPD. Enfin, les lignes directrices définissent les exigences relatives à un contrôle effectif d'un code.

Lignes directrices 2/2019 concernant l'article 6 (1) (b) du RGPD dans le contexte des services en ligne
Ces lignes directrices concernent le traitement des données à caractère personnel au titre de l'article 6(1)(b) du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées. Le concept de « nécessité » tel qu'il s'applique à « nécessaire à l'exécution d'un contrat » est analysé en détail dans les lignes directrices.

Lignes directrices 3/2019 sur le traitement des données à caractère personnel par des appareils vidéo
Des recommandations sur la manière d'appliquer le RGPD en ce qui concerne le traitement des données à caractère personnel par le biais d'appareils vidéo sont données dans ces lignes directrices de l'EDPB. Les exemples ne sont pas exhaustifs mais le raisonnement général peut être appliqué à tous les domaines d'utilisation potentiels.

Lignes directrices 4/2019 sur l'article 25 du RGPD : Protection des données dès la conception et protection des données par défaut
Ces lignes directrices donnent des orientations générales sur les obligations de protection des données prévues à l'article 25 du RGPD où l'obligation essentielle est la mise en œuvre dès la conception et la protection des données par défaut des principes de protection des données et des droits des personnes concernées. Cela exige que les responsables du traitement mettent en œuvre des mesures techniques et organisationnelles appropriées, assorties des garanties nécessaires. Ils doivent également être en mesure de démontrer l'efficacité des mesures mises en œuvre.

Lignes directrices 5/2019 sur le critère du droit à l'oubli dans les cas de moteurs de recherche dans le cadre du RGPD
Suite à l'arrêt Costeja de la Cour de justice de l'Union européenne du 13 mai 2014, une personne concernée peut demander au fournisseur d'un moteur de recherche en ligne d'effacer un ou plusieurs liens vers des pages web de la liste des résultats affichés à la suite d'une recherche effectuée sur la base de son nom.

Suite à l'arrêt de la CJUE, les autorités de contrôle ont constaté une augmentation du nombre de plaintes concernant le refus des fournisseurs de moteurs de recherche de supprimer des liens.

Ces lignes directrices visent à interpréter le droit à l'oubli dans les affaires relatives aux moteurs de recherche à la lumière des dispositions de l'article 17 du RGPD (Droit à l'effacement / « droit à l'oubli »).

Avis 3/2019 sur les questions et réponses concernant l'interaction entre le règlement sur les essais cliniques et le RGPD
Suite à une demande de la Commission européenne (DG SANTE), le Comité Européen de la Protection des Données a adopté un avis sur les questions et réponses relatives aux essais cliniques. L'avis aborde notamment les aspects liés aux bases juridiques adéquates dans le contexte des essais cliniques et aux utilisations secondaires des données d'essais cliniques à des fins scientifiques. L'avis était transmis à la Commission européenne.

Le règlement « vie privée et communications électroniques »
L'EDPB a adopté un avis sur l'interaction entre la directive ePrivacy et le règlement général sur la protection des données.

Dans la « Déclaration 3/2019 sur un règlement vie privée et communications électroniques », l'EDPB a par ailleurs invité les législateurs de l'UE à intensifier leurs efforts en vue de l'adoption d'un règlement « vie privée et communications électroniques », qui est nécessaire pour compléter le cadre de l'UE applicable en matière de protection des données et de confidentialité des communications.

Il a rappelé les positions précédemment adoptées par les autorités de protection des données dans l'UE, notamment l'avis 1/2017 du groupe de travail « article 29 » et la déclaration adoptée le 25 mai 2018. Selon l'EDPB, le règlement « vie privée et communications électroniques » ne doit en aucun cas abaisser le niveau de protection offert par l'actuelle directive 2002/58/CE relative à la vie privée et aux communications électroniques et doit compléter le RGPD en fournissant de solides garanties supplémentaires pour tous les types de communications électroniques. Loin de constituer un obstacle au développement de nouvelles technologies et de nouveaux services, le règlement « vie privée et communications électroniques » est nécessaire pour garantir des conditions de concurrence équitables et la sécurité juridique pour les opérateurs du marché.

L'EDPB a invité les États-membres, sous la direction de la présidence du Conseil, à assurer un niveau élevé de protection et à arrêter définitivement leur position de négociation, sans plus tarder, de sorte que les négociations avec le Parlement européen puissent commencer dans les meilleurs délais.

3.2 LE « GROUPE DE BERLIN »

Le Groupe de travail international sur la protection des données dans les télécommunications, mieux connu sous le nom de « Groupe de Berlin », se penche surtout sur la problématique de la protection de la vie privée dans les services de télécommunications et sur Internet.

Lors d'une réunion en 2019 à Bled (Slovénie), le groupe a adopté des documents de travail sur :

- les dispositifs intelligents (« smart devices ») pour les enfants et
- les services en ligne pour les enfants.

Ces documents peuvent être téléchargés dans leur intégralité (en anglais et en allemand) sur le site Internet du groupe de travail[6].

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

L'autorité de protection des données de la Géorgie a organisé la « Spring conference » à Tbilisi du 8 au 10 mai 2019.

Les thèmes suivants ont notamment été abordés lors de la conférence intitulée *« GDPR – One Year (G)old Standard »* :

- la modernisation de la Convention 108 ;
- la protection des données des enfants ;
- les activités des sous-groupes ;
- la protection des données et les organisations internationales ;
- le futur de la Conférence de printemps.

3.4 CONFÉRENCE INTERNATIONALE DES COMMISSAIRES DE LA PROTECTION DES DONNÉES

La 41e conférence internationale des commissaires de la protection des données a eu lieu du 21 au 24 octobre 2019 à Tirana (Albanie). Le thème de la conférence était *« Convergence and connectivity: raising global data protection standards in the digital age »*.

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

LES ACTIVITÉS EN 2019

3

Lors de la séance à huis clos les membres se sont entendus sur un cadre qui continue à renforcer la position du groupe en tant que forum international.

Les trois priorités stratégiques de la conférence sont de :

- faire progresser la protection de la vie privée dans le monde à l'ère du numérique ;
- maximiser la voix et l'influence de la conférence, notamment en renforçant le rôle de la conférence dans la politique numérique et les relations avec d'autres organismes et réseaux internationaux ;
- renforcer les capacités pour aider les membres à partager leur expertise tout au long de l'année.

Les résolutions suivantes ont été adoptées :

- Résolution sur la promotion d'instruments pratiques nouveaux et à long terme et la poursuite des efforts juridiques en vue d'une coopération efficace en matière de répression transfrontalière ;

- Résolution sur le respect de la vie privée en tant que droit humain fondamental et condition préalable à l'exercice d'autres droits fondamentaux ;
- Résolution visant à soutenir et à faciliter la coopération réglementaire entre les autorités chargées de la protection des données et les autorités chargées de la protection des consommateurs et de la concurrence afin d'atteindre des normes claires et constamment élevées de protection des données dans l'économie numérique ;
- Résolution sur le rôle de l'erreur humaine dans les atteintes à la protection des données personnelles ;
- Résolution sur les médias sociaux et les contenus extrémistes violents en ligne.

Une décision d'envergure a été le changement de nom à partir du 15 novembre 2019 de « International Conference of Data Protection and Privacy Commissioners (ICDPPC) » en « Global Privacy Assembly (GPA) ».

Ce changement représente l'évolution de la conférence dont le but est de renforcer sa visibilité et sa position en tant qu'acteur effectif et influent au niveau international.

A la suite de la séance à huis clos s'est tenue la partie ouverte aux professionnels de la protection des données notamment organisations internationales, entreprises informatiques, cabinets de conseil, cabinets d'avocats etc.

Les prochaines conférences internationales auront lieu au Mexique en 2020 et en Nouvelle-Zélande en 2021.

3.5 LE SÉMINAIRE EUROPÉEN « CASE HANDLING WORKSHOP »

Le Contrôleur européen de la protection des données a organisé le séminaire européen « Case Handling Workshop » à Bruxelles le 28 novembre 2019.

Ce « workshop » a permis aux employés des autorités de protection des données européennes d'échanger leurs expériences pratiques en matière de traitement des plaintes et de promouvoir la coopération entre les différentes autorités.

Les thèmes suivants ont été abordés au cours des différentes sessions :

- les consultations préalables ;
- les courtiers en données et les systèmes de référence de crédit ;
- le traitement des affaires transfrontalières ;
- les pratiques d'enquête et
- la détermination des mesures correctrices.

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

1 RAPPORT DE GESTION RELATIF AUX COMPTES DE L'EXERCICE 2019

Dépenses

L'année 2019 a été une année de renforcement et de consolidation des structures mises en place auprès de la Commission nationale pour la protection des données (CNPD) dans le cadre de l'entrée en application le 25 mai 2018 du nouveau règlement européen pour la protection des données (RGPD).

La loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données a donné une nouvelle base légale à la CNPD (ci-après « la loi du 1er août 2018 »), lui permettant d'exécuter toutes les tâches et missions que le RGPD prévoit pour elle.

Alors que les travaux de guidance et de sensibilisation pour aider les acteurs concernés à se mettre en conformité à l'arrivée du RGPD étaient la préoccupation majeure de tous les membres du personnel de la CNPD au cours de l'année 2018, l'élaboration et la mise en place de nouvelles structures internes ainsi que l'adoption d'un nouvel organigramme afférent, d'autre part, marquaient l'année 2019.

Si la loi du 1er août 2018 a continué la personnalité juridique, y compris le personnel et les engagements juridiques de la Commission nationale pour la protection des données (instituée initialement par l'ancienne loi du 2 août 2002), elle a aussi procédé à des modifications au niveau de l'organisation de la CNPD en prévoyant, entre autres, le renfort du collège par un quatrième Commissaire et la nomination d'un réviseur d'entreprise agréé. Les comptes de 2018 étaient ainsi les premiers à être audités par un réviseur d'entreprises, lequel a émis un rapport favorable à cet égard.

Le budget de la CNPD pour 2019 de 5.442.516 € était marqué par les efforts de renforcement des ressources humaines de la CNPD. Bien que la progression de 24% par rapport au budget de l'année de 2018 qui s'élevait à 4.415.419 € n'était pas aussi forte que la progression de l'année précédente qui était de 85 %, elle était tout de même substantielle et a permis à la CNPD de poursuivre sa stratégie de développement 2015-2019.

Tout comme l'année précédente, les fonds supplémentaires étaient essentiellement destinés au recrutement d'effectifs additionnels et à couvrir les frais de fonctionnement occasionnés par une commission en expansion.

Le total des frais de fonctionnement de l'établissement public au cours de l'exercice 2019 s'élevait à 4.799.183 € ce qui constitue une augmentation de 33% par rapport à l'exercice précédent qui s'élevait à 3.604.309 €.

Le total des frais de fonctionnement restait toutefois en dessous du montant des prévisions budgétaires originaires estimées à 5.442.516 €.

La différence de 643.333 € s'explique essentiellement par deux positions, à savoir les moins-values pour charges relatives au personnel, d'une part, et pour les frais de location pour les nouveaux locaux de la CNPD, d'autre part.

En effet, pour ce qui est des charges relatives au personnel permanent et temporaire, celles-ci avaient certes augmenté sensiblement, pour atteindre 4.362.465 € en 2019, comparées à 3.106.940,50 € en 2018. Or, les dépenses réelles sont restées en dessous des prévisions budgétaires initialement estimées à 4.612.062 €, soit de 5,4 %. Au cours de l'année 2019, les effectifs de la CNPD ont pu être augmentés de 9 personnes et un quatrième commissaire est entré en fonction le 1er mai 2019. En fin d'année, l'effectif de la CNPD s'élevait à 43 unités. Les engagements se composaient de 9 employés de la carrière A1, dont 6 employés de l'État engagés à plein temps à durée indéterminée et 3 employés de l'État engagés à plein temps à durée déterminée. Dans la même période, le statut de 2 employés de l'État de la carrière A1 a été converti en celui de fonctionnaires suite à la réussite de l'examen-concours par les intéressés.

A noter que pendant l'année entière, un fonctionnaire de la carrière B1 a continué à bénéficier d'un congé pour travail à mi-temps pour des raisons médicales et qu'un autre était absent pour des raisons de maladie. Étant donné que la CNPD ne peut pas bénéficier de la provision globale de l'Etat pour remplacements, elle assume elle-même les frais pour ces absences.

Une moins-value de 111.214,37 € sur la somme estimée de 266.000 € était relative à un contrat de location pour un nouveau siège pour la CNPD qui avait été signé avec quelques mois de retard. En raison de l'augmentation de ses effectifs, une relocation du personnel de la CNPD dans des locaux où tous les membres du personnel sont réunis est devenue indispensable pour garantir le bon fonctionnement et la bonne coopération entre ses services. Le montant des charges locatives pour le bâtiment administratif à Belval et la partie des charges locatives pour les nouveaux locaux s'élevait à 41.134,21 €.

Pour ce qui était des charges pour la gestion et la maintenance des systèmes et réseaux informatiques, la CNPD, consciente que ses rôles et responsabilités allaient fortement évoluer avec l'arrivée du RGPD, a dû investir pour informatiser de manière systématique ses procédures de travail existantes et futures. Pour relever les défis et assurer un service efficace de haute qualité, la CNPD avait opté pour une digitalisation poussée. Dans cette perspective, la CNPD avait réorienté le modèle opérationnel de son service informatique. Ainsi, la CNPD a depuis 2018 recours à un service de type Plateforme As A Service (Cloud), dont le prestataire est le CTIE. Selon le prix du marché, le service offert équivalait à 308.240,07 €. En 2018, la facture ne s'élevait toutefois qu'à 62.663 €. Cette différence s'explique par le fait que la CNPD a pu développer sa nouvelle plateforme de travail « SharePoint » en utilisant exclusivement des composantes standards du CTIE. De ce fait, le système de la CNPD peut être opéré sur une plateforme standard et mutualisé du CTIE – réduisant ainsi fortement les coûts. En 2019, une somme de

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

190.513 € avait été prévue pour couvrir les frais afférents, mais la facture n'avait pas encore été adressée à la CNPD à la clôture de l'exercice. Un montant de 54.405 € avait par ailleurs été déboursé relatif à l'hébergement par une société spécialisée de l'outil « CNPD Compliance Support Tool », développé par la CNPD en coopération avec le LIST (Luxembourg Institute of Science and Technology) et le Service des Médias et des Communications par une société spécialisée.

D'autres postes substantiels étaient constitués par les frais d'honoraires estimés à 24.000 € pour couvrir les frais de la fiduciaire, les frais pour le personnel de remplacement et une provision pour honoraires d'avocat. Un montant de 19.353 € a été dépensé pour payer les frais de comptabilité de la fiduciaire ainsi qu'une avance pour le réviseur d'entreprises agréé.

Les frais de port et de télécommunications ont connu une légère baisse, alors que depuis le 25 mai 2018, la CNPD n'émet plus d'autorisations et n'accuse plus réception de notifications et par conséquent, envoie moins de courriers postaux. Ils ne s'élevaient qu'à 11.418 € comparés à 12.467 € en 2018. Les autres charges générales d'exploitation ont connu une progression linéaire suivant l'augmentation du nombre de collaborateurs en activité.

Pour ce qui est des équipements et fournitures de bureau, les dépenses ont diminué de 60% pour tomber de 28.056 € en 2018 à 17.517 € en 2019. Cette baisse s'explique par le fait que la CNPD devait seulement équiper quelques bureaux en attendant son déménagement vers ses nouveaux locaux. Les frais y relatifs figurent au tableau d'amortissement.

Les frais de déplacement et de séjour à l'étranger en 2019 se chiffraient à 61.238 € ce qui constitue une progression de 25 % par rapport à la dépense de l'année précédente qui s'élevait à 48.826,77 €. Cette progression qui dépasse par ailleurs largement les prévisions de 42.000 € s'explique par le nombre élevé de réunions en rapport avec le mécanisme de cohérence et de coopération européen mis en place par le RGPD.

Les frais de formation externe, hors frais de déplacement et de séjour, pour le personnel ont par contre connu une importante baisse en 2019 pour ne s'élever qu'à 1.050,51 € sur les 17.150 € initialement estimés. C'est une baisse de 96 % par rapport à la dépense de l'année précédente de 26.209,30 €. Cette baisse s'explique par le fait que la majorité des agents ont effectué leurs formations à l'Institut national d'administration publique qui dispense depuis 2019 ce type de cours gratuitement pour les agents de l'État. Ainsi la CNPD n'a pas eu besoin d'engager elle-même des frais pour des cours de langue en 2019. Or, la tendance est actuellement au congé linguistique ce qui veut dire que les dépenses pour l'apprentissage de la langue luxembourgeoise, auquel la CNPD attache une grande importance, se répercuteront dorénavant sur les frais du personnel.

Les dépenses relatives à l'information du grand public et la communication ne s'élevaient qu'à 29.678,94 € en 2019, ce qui est une baisse significative par rapport à la dépense de l'année précédente de 102.699,41 € essentiellement liées aux actions de sensibilisation autour de l'entrée en application du RGPD. Pour 2019, les dépenses sur cette position n'avaient été estimées qu'à 8.000 € en attendant que la CNPD redéfinisse sa stratégie de communication et de sensibilisation.

Les amortissements comptabilisés en 2019 atteignaient un montant total de 23.365,49 € comparé à 16.111,56 € en 2018. Cette augmentation est essentiellement due à l'acquisition au cours de l'année 2018, d'un logiciel comptable, d'un côté, et de nouveau mobilier destiné à accueillir les nouveaux membres du personnel de la CNPD, de l'autre.

Recettes
Jusqu'au 25 mai 2018, la CNPD émettait des autorisations et recevait des notifications conformément aux dispositions de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Depuis l'abrogation de cette loi, la CNPD n'a pas généré de recettes propres.

Résultat d'exploitation
Compte tenu de la dotation annuelle de 5.442.416 €, dont la Commission nationale a bénéficié pour l'exercice 2019 de la part de l'Etat en application de l'article 37 paragraphe (4) de la loi du 2 août 2002 précitée, le résultat d'exploitation de l'établissement public s'élève à 643.233 € au 31 décembre 2019.

Le rapport de gestion relatif aux comptes de l'exercice 2019 a été adopté le 27 mai 2020 par les quatre Commissaires.

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

2 PERSONNEL ET SERVICES

Collège
Tine A. LARSEN, Présidente

Thierry LALLEMANG, Commissaire

Christophe BUSCHMANN, Commissaire

Marc LEMMER, Commissaire

Dani JEITZ, Attachée,
Secrétariat du Collège « Formation plénière »

Claudia FETZ, Employée A1,
Secrétariat du Collège « Formation restreinte »

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

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

Marc HEMMERLING, Association des Banques
et Banquiers Luxembourg (ABBL),
membre du comité de direction

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

Data Protection Officer
Bertrand NAVARRE, Employé A1,
Délégué à la protection des données

Relation internationales
Romy SCHAUS, Attachée,
Chargée aux relations internationales

Service Administration
Tine A. LARSEN, Présidente

Irena ADROVIC, Chef de service

Maryse WINANDY, Chef d'unité,
Réception/Secrétariat

Jan KUFFER, Employé A2, IT interne & Logistique

Anna MAGI, Employée, Ressources humaines,
Comptabilité et Finances

Stéphanie MATHIEU, Rédacteur, Secrétariat

Service Sensibilisation
Marc LEMMER, Commissaire

Tom KAYSER, Chef d'unité, Communication externe

Alexandre KUHN, Employé A1,
Veille juridique et technologique

Vincent LEGELEUX, Attaché,
Veille juridique et technologique

Service Guidance
Thierry LALLEMANG, Commissaire

Arnaud HABRAN, Chef de service

Francis MAQUIL, Chef d'unité, Conseil juridique

Carmen SCHANCK, Chef d'unité, Avis juridiques

Mathilde STENERSEN, Chef d'unité,
Ligne directrices thématiques

Sabrine ABAAB, Employée A1, Conseil juridique

Clémentine BOULANGER, Employée A1,
Avis juridique

Nina BURMEISTER, Attachée, Conseil juridique

Marie DOUZAL, Employée A1, Conseil juridique, Avis juridiques

Kalliroi GRAMMENOU, Employée A1, Conseil juridique, Avis juridiques

Christian WELTER, Conseiller, Conseil juridique, Avis juridiques

Service Conformité
Marc LEMMER, Commissaire

Alain HERRMANN, Chef de service

Christine ANDRES, Employée A1, Certification

Service Réclamations
Thierry LALLEMANG, Commissaire

Laurent MAGNUS, Chef de service,

Georges WEILAND, Chef d'unité, réclamations européennes

Sabrine ABAAB, Employée A1, réclamations européennes

Solène BENNET, Employée A1, réclamations nationales et européennes

Clémentine BOULANGER, Employée A1, réclamations nationales

Gaël DUMORTIER, Employé A1, réclamations nationales

Barbara Giroud, Employée A1, réclamations nationales et européennes

Stéphanie MATHIEU, Rédacteur, réclamations européennes

Nicolas RASE, Employé A1, réclamations nationales et européennes

Service Enquêtes
Christophe BUSCHMANN, Commissaire

Michel SINNER, Chef de service, Chef d'unité Contrôle

Edith MALHIERE, Chef d'unité, Audits

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

Christine ANDRES, Employée A1, Audits, Notifications de violations de données

Jérôme COMMODI, Employé A1, Contrôles

Marie-Laure FABBRI, Employée A1, Audits

Alexandre KUHN, Employé A1, Contrôles

Vincent LEGELEUX, Attaché, Audits

Marc MOSTERT, Inspecteur, Contrôles

François RICHALET, Employé A1, Audits

Mathieu RINCK, Employé A1, Audits

Céline SIMON-HERTZ, Employée A1, Contrôles

Maximilian WELSCH, Employé A1, Contrôles

RESSOURCES, STRUCTURES ET FONCTIONNEMENT

4

2.1 NOUVELLES NOMINATIONS EN 2019

Le 8 mars 2019, le Conseil de gouvernement a proposé la nomination de Monsieur Marc Lemmer comme Commissaire à la protection des données.

Marc Lemmer a rejoint la Commission nationale pour la protection des données à partir du 1er mai 2019. Son expérience professionnelle en matière d'innovation, de digitalisation et d'entrepreneuriat tout comme dans le conseil, le contrôle et la certification permettra à la CNPD de continuer et d'accélérer son développement dans l'intérêt du droit fondamental de la protection des personnes physiques à l'égard des données à caractère personnel, ainsi que dans l'intérêt de la libre circulation de ces données.

Le Conseil de gouvernement a également proposé la nomination de Madame Martine Kraus en tant que membre suppléant du Collège de la CNPD. Madame Martine Kraus, de formation juriste, a exercé en tant qu'avocate à la cour avant de rejoindre la magistrature en 2004.

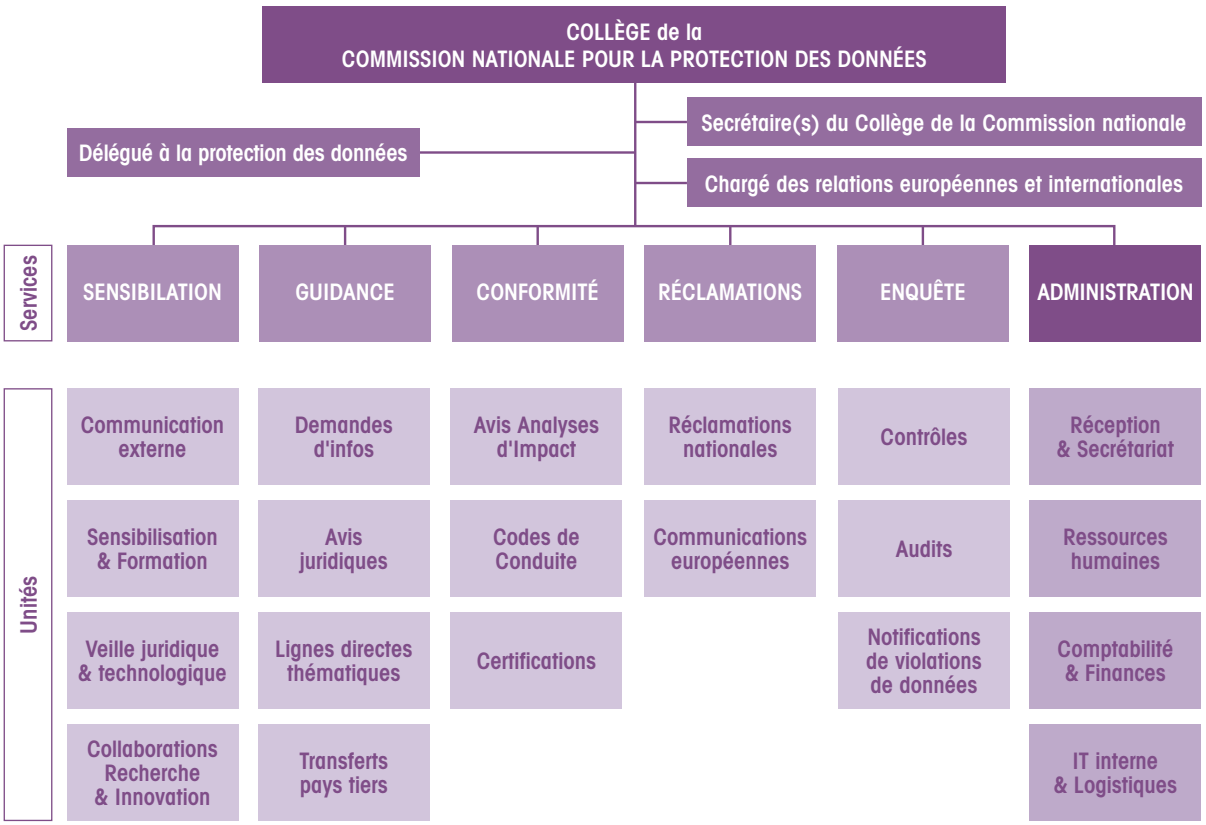
Les postes d'un quatrième commissaire et d'un quatrième membre suppléant du Collège de la CNPD ont été créés par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. Cette loi a été adoptée dans le contexte de la mise en application du Règlement général sur la protection des données de l'Union européenne entré en vigueur le 25 mai 2018.

Par arrêté grand-ducal du 19 novembre 2019, Madame Michèle Bram, Directrice adjointe à l'Institut luxembourgeois de régulation, a été nommée membre suppléant de la CNPD pour une durée de six ans, en remplacement de Madame Josiane Pauly, membre suppléant démissionnaire.

3 ORGANIGRAMME DE LA CNPD

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

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



ANNEXES

5

5 ANNEXES

AVIS ET DÉCISIONS

ANNEXES

5

ANNEXES

5

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal portant exécution de la loi du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs.

Délibération n°9/2019 du 17 janvier 2019

Conformément à l'article 57, paragraphe 1er, lettre (c) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

En date du 28 novembre 2018, la CNPD a avisé le projet de loi n°7217 instituant un Registre des bénéficiaires effectifs et portant 1° transposition des dispositions de l'article 30 de la directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n°648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, telle que modifiée par la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018; 2° modification de la loi modifiée du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises ainsi que le projet de règlement grand-ducal portant exécution de la loi du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs.

La loi du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs était publiée au Journal officiel du Grand-duché de Luxembourg en date du 15 janvier 2019.

En date du 11 janvier 2019, Monsieur le Ministre de la Justice, Félix Braz, a transmis à la CNPD un amendement au projet de règlement grand-ducal portant exécution de la loi du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs.

L'amendement concerne l'article 5 du projet de règlement grand-ducal, plus précisément les pièces justificatives qui doivent accompagner la demande d'inscription. Suite à l'amendement, les entités immatriculées ne seront plus obligées de transmettre une copie de la pièce d'identité des personnes concernées, dont les données seraient

conservées par le registre des bénéficiaires effectifs, si ces dernières disposent d'un numéro d'identification tel que prévu par la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques. Cet amendement vise ainsi à adresser les remarques faites par la CNPD dans son avis du 22 novembre 2018 relatif au projet de loi n°7217 (délibération n°485/2018). Or, une pièce d'identité doit être fournie pour les personnes concernées ne disposant pas d'un tel numéro d'identification. Le commentaire de l'amendement n'adresse pas les interrogations de la CNPD relatives à la nécessité en général de l'obtention et de la conservation de cette pièce d'identité. Il conviendrait dès lors de le préciser.

Par ailleurs, la CNPD regrette que les auteurs du projet de règlement grand-ducal n'ont pas jugé opportun de modifier d'autres dispositions du texte, notamment celles concernant les données à caractère personnel figurant au registre (cf. sections II et IV. de l'avis de la CNPD du 22 novembre 2018), les modalités d'accès au registre, y compris l'acquittement des frais, les modalités de recherche, les mesures de sécurité et les mesures visant à prévenir des abus (cf. section V. de l'avis de la CNPD du 22 novembre 2018), ainsi que la durée de conservation des données (cf. section VI. de l'avis de la CNPD du 22 novembre 2018).

En effet, en réglant l'accès au registre, sans prévoir des garanties cherchant à limiter l'impact considérable qu'aura ce registre sur les des droits fondamentaux des personnes concernées, le projet de règlement grand-ducal, dans son état actuel, risquerait d'être contraire au RGPD en n'étant pas limité à ce qui est approprié et nécessaire à la réalisation des objectifs légitimes poursuivis par la réglementation en cause et n'assurerait pas une transposition fidèle de la Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, telle que modifiée par la Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/CE.

Afin de trouver un juste équilibre *« entre l'intérêt du grand public à la prévention du blanchiment de capitaux et du financement du terrorisme et les droits fondamentaux des personnes concernées »,* comme envisagé par la Directive 2018/843 (considérant 34 de la Directive 2018/843), et pour assurer la conformité du cadre légal luxembourgeois au RGPD, la CNPD estime nécessaire de modifier le projet de règlement grand-ducal afin d'intégrer les remarques faites par la CNPD dans son avis du 22 novembre 2018.

Ainsi décidé à Esch-sur-Alzette en date du 17 janvier 2019.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Marc Hemmerling Membre suppléant

ANNEXES

5

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7348 relative aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence et modifiant : 1. la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et 2. la loi modifiée du 7 décembre 2015 sur le secteur des assurances.

Délibération n°10/2019 du 1er février 2019

Conformément à l'article 57, paragraphe 1er, lettre (c) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

Faisant suite à la demande lui adressée par Monsieur le Ministre des Finances en date du 3 août 2018, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n°7348 relative aux comptes inactifs, aux coffres-forts inactifs et aux contrats d'assurance en déshérence et modifiant : 1. la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et 2. la loi modifiée du 7 décembre 2015 sur le secteur des assurances (ci-après « le projet de loi »).

Selon l'exposé des motifs, le projet de loi vise à instaurer en droit luxembourgeois un cadre légal régissant les comptes et coffres-forts inactifs et les contrats d'assurance tombés en déshérence. Il instaure l'obligation pour les établissements de crédit, tel que défini à l'article 1er, point 8. du projet de loi, et les entreprises d'assurance de maintenir un contact régulier avec leurs clients et de les contacter et, si nécessaire, d'entreprendre des recherches complémentaires en cas d'absence de manifestation de la part des clients. Pour le cas où l'inactivité du client se poursuit jusqu'au délai fixé dans le projet de loi, les établissements et entreprises d'assurance devraient consigner les avoirs des clients auprès de la Caisse de consignation.

Le projet de loi encadre encore les missions des acteurs chargés de veiller à l'application du projet de loi, à savoir la Commission de surveillance du secteur financier (« la CSSF »), le Commissariat aux assurances (« le CAA »), l'Administration des contributions directes (« l'ACD ») et la Caisse de consignation.

La Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de loi sous examen traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel.

I. Les traitements de données à caractère personnel effectués par les établissements et les entreprises d'assurances

a. Les données à caractère personnel traitées par les établissements et les entreprises d'assurances

i. Au cours de la relation contractuelle

Au cours de la relation contractuelle, les établissements et les entreprises d'assurance doivent tenir à jour les données qu'ils détiennent sur leurs clients (articles 4 et 19 du projet de loi).

A cette fin, les établissements et les entreprises d'assurance doivent, dans les délais fixés par le projet de loi, contacter les personnes concernées (p.ex. le titulaire du compte ou l'ayant droit pour les établissements, l'assuré pour les entreprises d'assurance) *« par tout moyen »*, en ayant recours *« aux données à leur disposition »* (voir, entre autres, article 5, paragraphe 1er, alinéa 2 et article 20, paragraphe 1er, alinéa 2 du projet de loi). Selon le commentaire des articles, sont visées *« toutes [les] données dont l'établissement dispose, telle que les adresses privées ou professionnelles, les numéros de téléphones ou de fax, privés ou professionnels, les adresses email dont l'établissement dispose ou encore la transmission de messages par web-banking »*[1].

A défaut de manifestation des personnes concernées, les établissements (pour les comptes inactifs) et les entreprises d'assurance doivent procéder à des recherches complémentaires afin de rétablir le contact avec les personnes concernées[2]. La CNPD salue la précision dans le commentaire des articles selon laquelle : *« les données obtenues suite aux recherches complémentaires ne peuvent être utilisées que pour les besoins de la présente loi »* [3]. La CNPD tient à souligner qu'en vertu du principe de minimisation des données, seules les informations issues des recherches complémentaires qui ont permis de rétablir le lien avec le client ou les données actualisées que les personnes ont fourni devraient être conservées par les entreprises, à l'exclusion de toutes autres données non-pertinentes ou dont l'exactitude n'a pas pu être vérifiée. Dans la mesure où le contact n'a pas pu être rétabli, les preuves démontrant l'accomplissement des recherches complémentaires doivent être conservées pendant le délai prévu par le projet de loi (article 6, paragraphe 2, alinéa 3 er article 22, paragraphe 2, alinéa 3 du projet de loi). Ces preuves doivent être limitées à ce qui est strictement nécessaires pour démontrer le respect des dispositions du présent projet de loi.

ii. Lors de la consignation

L'article 29, paragraphe 2 de la loi en projet dispose que les informations et documents visés à l'annexe 3 sont conservés pendant toute la durée de la consignation et pendant cinq ans suivant la date à laquelle la consignation

[1] Projet de loi n°7348, doc. parl. 7348/00, Commentaire des articles, p. 45 pour les établissements et p. 55-56 pour les entreprises d'assurance.
[2] Projet de loi n°7348, doc. parl. 7348/00, Commentaire des articles, p. 47.
[3] Projet de loi n°7348, doc. parl. 7348/00, Commentaire des articles, p. 48 et 57.

a pris fin, *« afin de permettre à la Caisse de consignation d'examiner les demandes d'information au titre de l'article 32, d'examiner les demandes de restitution et de procéder aux restitutions au titre de l'article 33 »*. Les établissements et les entreprises d'assurance doivent en plus conserver les pièces justificatives issues des recherches complémentaires pour justifier aux personnes concernées et aux organismes public de l'accomplissement de leurs obligations légales[4].

L'annexe 3 du projet de loi énonce à cet égard les informations que les établissements et les entreprises d'assurance doivent conserver pendant la durée de la consignation. Sont ainsi visées *« les informations et la documentation pertinentes pour l'identification, … y compris les informations et la documentation requises conformément à la loi modifiée du 12 novembre 2004 [relative à la lutte contre le blanchiment et contre le financement du terrorisme] »*. Les informations requises conformément à la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (ci-après « la loi modifiée du 12 novembre 2004 ») incluent *« une copie ou les références des documents, des données et informations qui sont nécessaires pour se conformer aux obligations de vigilance à l'égard de la clientèle »*[5], ainsi que *« les pièces justificatives et enregistrements de transactions qui sont nécessaires pour identifier ou reconstituer des transactions »*[6]. Le commentaire des articles ne précise pas pourquoi ces données seraient nécessaires.

La conservation de toutes les données collectées sur base de la loi modifiée du 12 novembre 2004 risquerait de ne pas être proportionnelle par rapport à l'objectif du projet de loi, puisque les établissements et les entreprises d'assurance seraient obligées de conserver l'entièreté des dossiers de leurs clients établis sur base de la loi modifiée du 12 novembre 2004. Dans la mesure où les données collectées conformément à la loi modifiée du 12 novembre 2004 ne doivent être conservées au-delà de dix ans maximum après la fin de la relation contractuelle[7], le projet de loi dans sa rédaction actuelle pourrait avoir comme conséquence de prolonger la durée de conservation desdites données pour une durée disproportionnée eu égard à la finalité initiale de la collecte.

Étant donné que le but de la conservation des données est *« de permettre à la Caisse de consignation d'examiner les demandes d'information au titre de l'article 32, d'examiner les demandes de restitution et de procéder aux restitutions au titre de l'article 33 »*, la CNPD estime nécessaire de limiter les données conservées aux seules données d'identification.

b. <u>La durée de conservation</u>

Quant à la durée maximale de conservation de données, la CNPD note que les points de départs précis pour les délais de prescription varient en fonction des avoirs et des biens en question.

Ainsi, si la demande de consignation est acceptée, le délai de prescription trentenaire pour les avoirs provenant des comptes bancaires et des coffres-forts inactifs, ainsi que des contrats d'assurance en déshérence commence à

[4] Projet de loi n°7348, doc. parl. 7348/00, Commentaire des articles, p. 48 et 57.
[5] Article 3, paragraphe 6, alinéa 1er, lettre a de la loi modifiée du 12 novembre 2004.
[6] Article 3, paragraphe 6, alinéa 1er, lettre b de la loi modifiée du 12 novembre 2004.
[7] Article 3, paragraphe 6 de la loi modifiée du 12 novembre 2004.

courir à partir du point de départ de l'inactivité (article 37, paragraphe 1er, point 1er du projet de loi). Les données relatives à ces consignations devront être conservées pendant la durée de la consignation et 5 ans après la fin de la consignation, à savoir pendant une durée maximale de 35 ans à partir du point de départ de l'inactivité (article 29, paragraphe 2 du projet de loi).

Pour les biens dont l'établissement reste dépositaire, à savoir *« les biens non visés aux paragraphes 2 à 7 [de l'article 15 du projet de loi], qui sont conservés dans une enveloppe scellée »*, ne seront consignés auprès de la Caisse de consignation qu'après 50 ans à partir du point de départ de l'inactivité (article 15, paragraphe 8 du projet de loi). Le délai de prescription est de cinq ans après la délivrance du récépissé de consignation par la caisse de consignation (article 37, paragraphe 1er, point 2. du projet de loi). Les données relatives à ces biens devront ainsi être conservées pendant une durée maximale de 10 ans après la délivrance du récépissé de consignation.

La CNPD s'interroge sur la durée de conservation des données, si la demande est refusée (soit implicitement, soit expressément). Qu'en-est-il de la conservation en cas de refus de la demande (de manière implicite et expresse) : est-ce que les responsables du traitement doivent garder les avoirs et les données y afférentes *ad vitam aeternam* ? La CNPD estime nécessaire de préciser davantage le projet de loi à cet égard.

La CNPD rappelle encore que les données devraient être effacées à la fin de la durée de conservation prescrite par la présente loi en projet, étant donné qu'elles ne doivent pas être conservées plus longtemps que la durée pendant laquelle elles sont nécessaires au regard des finalités pour lesquelles elles sont traitées (article 5, paragraphe 1er, lettre (e) du RGPD).

c. <u>L'information annuelle et la transmission de la demande de consignation</u>

Selon l'article 27 du projet de loi, les établissements transmettent le nombre total de titulaires de comptes inactifs et coffres-forts, le nombre total desdits comptes inactifs et desdits coffres-forts inactifs, ainsi que le solde global de tous les comptes inactifs à la CSSF et à l'ACD. Les entreprises d'assurance, quant à elles, sont tenues de transmettre à la CAA et à l'ACD le nombre total de contrats d'assurance en déshérence et le solde global desdits contrats en déshérence.

Le commentaire des articles précise que la transmission de données à la CSSF et le CAA se ferait pour assurer le *« suivi de l'évolution des comptes et coffres-forts inactifs ainsi que des contrats d'assurance en déshérence à des fins statistiques et de surveillance, notamment dans le cadre de l'analyse des risques liés au blanchiment des capitaux »*[8]. Les transmissions à l'ACD auraient lieu dans le cadre de l'application de la loi du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) ainsi que la loi modifiée du 24 juillet 2015 relative à FATCA pour permettre au *« bureau de la retenue d'impôt sur les intérêts [de contrôler] le respect des obligations incombant aux établissements et aux entreprises d'assurance envers l'Administration des contributions directes*

[8] Projet de loi n°7348, doc. parl. 7348/00, Commentaire des articles, page 59.

conformément aux paragraphes 1er et 2 » (article 27, paragraphe 3 du projet de loi). Le commentaire des articles explique que *« dans les deux cas visés aux paragraphes 1er et 2, il y aura une transmission unique d'un même jeu de données à la fois à la CSSF et à l'ACD, respectivement au CAA et à la l'ACD »*[9].

Tel que l'article 27 du projet de loi est libellé, la CNPD comprend que les informations sont transmises à la CSSF, le CAA et l'ACD sous forme agrégée, même si la disposition ne le précise pas expressément. Si les informations agrégées ne permettent plus d'identifier une personne physique de manière directe ou indirecte, on pourrait considérer qu'il s'agisse de données anonymes de sorte que la législation sur la protection des données ne trouverait pas application.

Par ailleurs, afin d'assurer la conformité du projet de loi avec l'article 5, paragraphe 1er, lettre (c) du RGPD, le mot « utiles » devrait être remplacé par « nécessaires » à l'article 28, paragraphe 2, alinéa 1er du projet de loi.

II. Les traitements de données à caractère personnel effectués par la Caisse de consignation, la CSSF, le CAA et l'ACD

a. Les rôles et responsabilités

L'article 32 du projet de loi vise à encadrer le registre électronique des consignations tenu par la Caisse de consignation. Dans un souci de sécurité juridique, il importe, le cas échéant, de préciser que la Caisse de consignation est à considérer comme le responsable du traitement au sens du RGPD.

b. Les données traitées par la Caisse de consignation

Le projet de loi n'énumère pas dans une disposition unique les données qui sont collectées par la Caisse de consignation. Il ressort du projet de loi que la Caisse de Consignation traiterait les données transmises par les établissements et les entreprises d'assurance dans le cadre de la demande de consignation (annexes 1 et 2 du projet de loi), dont notamment *« les informations relatives aux »* personnes concernées par la demande, à savoir les titulaires, ayants-droit, preneurs d'assurance, assurés et/ou bénéficiaires. La Caisse de consignation peut encore demander *« toutes les informations et pièces supplémentaires utiles »* (article 28, paragraphe 2 du projet de loi) qu'elle juge nécessaires pour traiter la demande. Le commentaire des articles souligne à cet égard que la documentation conservée par les établissements et les entreprises d'assurance conformément à l'article 29 du projet de loi ne serait pas conservée par la Caisse de consignation[10].

La CNPD s'interroge ainsi sur le sort des informations et pièces supplémentaires transmises par les établissements et les entreprises d'assurance suite à une demande de la Caisse de consignation. S'agit-il de la documentation qui doit être conservée par les établissements et les entreprises d'assurance ? Est-ce que ces informations et pièces

[9] Ibid.
[10] Projet de loi n°7348, doc. parl. 7348/00, Commentaire des articles, page 61.

supplémentaires seront conservées en double ou est-ce qu'elles seront effacées par la Caisse de consignation suite à l'acceptation de la demande ?

La Caisse de consignation traiterait encore les informations fournies par les demandeurs dans le cadre de leur demande d'information et/ou de restitution. Elle peut à cet égard également demander *« toute information et pièce justificative supplémentaire »* des demandeurs et *« les informations et documents visés à l'annexe 3 qui sont utiles en vue de l'examen des demandes de restitution et des démarches de restitution »* (article 33, paragraphe 1er, alinéas 2 et 4 du projet de loi). Les établissements et les entreprises d'assurance devraient transmettre *« l'ensemble de la documentation conservée conformément à l'article 29, paragraphe 2, qui est en relation avec la demande de restitution examinée »* (article 33, paragraphe 1er, alinéa 5 du projet de loi). Il importe de modifier ces dispositions afin de limiter les données qui pourront être traitées par la Caisse de consignation.

Par ailleurs, dans un souci de clarté, la CNPD s'interroge s'il ne serait pas utile de prévoir de manière plus précise dans le corps du texte de l'article 32 le contenu du registre tenu par la Caisse de consignation.

c. La durée de conservation

La CNPD relève que le projet de loi n'énonce pas explicitement la durée de conservation des données à caractère personnel traitées par la Caisse de consignation, la CSSF, le CAA et l'ACD dans le cadre de leurs missions respectives au titre du présent projet de loi. Quant à la Caisse de consignation, la CNPD suppose que les données seraient effacées cinq ans après la fin de la consignation.

Il ressort de l'article 5, paragraphe 1er, lettre (e) du RGPD que les données ne doivent pas être conservées au-delà de la durée nécessaire au regard des finalités pour lesquelles elles sont traitées. Par ailleurs, la protection des données à caractère personnel constitue une matière réservée à la loi en ce qu'elle touche à la protection de la vie privée des citoyens (article 11, paragraphe 3 de la Constitution). Les éléments essentiels[11], les objectifs et les principes, dont notamment la durée de conservation[12], doivent dès lors figurer dans la loi.

Au vu de ce qui précède et dans un souci de sécurité juridique, la CNPD estime nécessaire de préciser les durées de conservation des données traitées par la Caisse de consignation, la CSSF, le CAA et l'ACD.

d. Les transferts de données à caractère personnel

i. La coopération entre la CSSF, le CAA et la Caisse de consignation

L'article 38 du projet de loi habilite la CSSF, le CAA et la Caisse de consignation à coopérer et à échanger des informations et documents *« aux fins de l'accomplissement de leurs missions respectives au titre de la présente loi »*.

[11] Arrêt de la Cour constitutionnelle - Arrêts n°00132 et 00133 du 2 mars 2018.
[12] Avis n°52976 du Conseil d'État du 24 juillet 2018 relatif au Projet de règlement grand-ducal 1. modifiant le règlement grand-ducal modifié du 10 août 2005 relatif au fonctionnement du lycée-pilote, et 2. abrogeant le règlement grand-ducal du 27 août 2012 portant sur les classes de la division supérieure de l'enseignement secondaire dans le cycle de formation du lycée Ermesinde.

Pour le cas où la coopération entre lesdits organismes comprenait des données à caractère personnel, la CNPD s'interroge sur la forme ou l'étendue de cette coopération.

En effet, toute base juridique servant de fondement à un traitement de données à caractère personnel visé à l'article 6, paragraphe 1er, lettres (c) (le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis) ou (e) (le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement) du RGPD, doit être accompagnée de garanties appropriées en matière de protection des données. En particulier, suivant le paragraphe 3 de ce même article :

« (…) les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (…) ».

Ces finalités doivent être déterminées, explicites et légitimes[14] et les données ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités (principe de limitation des finalités).

L'article 6, paragraphe 3 du RGPD prévoit encore que *« (…) cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX [du RGPD] (…) ».*

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

Il convient en outre de rappeler l'obligation d'information préalable prescrite aux articles 13 (collecte directe) et 14 (collecte indirecte) du RGPD. Ainsi, les responsables du traitement sont obligés de fournir certaines informations aux personnes concernées, dont notamment les catégories de données à caractère personnel concernées. L'obligation d'information préalable ne s'applique pas en cas de collecte indirecte dans des cas précis,

[14] PRGPD, article 5, paragraphe 1er, lettre (b).
[15] RGPD, article 14, paragraphe 5.
[16] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[17] Arrêt du 1er octobre 2015, Smaranda Bara, C-201/14, point 47.

par exemple, lorsque *« l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État-membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée »*[15].

Dans l'arrêt *« Smaranda Bara »* du 1er octobre 2015, la Cour de Justice de l'Union européenne a retenu que les articles de la directive 95/46/CE[16] relatives à l'obligation d'information préalable *« doivent être interprétés en ce sens qu'ils s'opposent à des mesures nationales … qui permettent à une administration publique d'un État-membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement »*[17]. La Cour a notamment considéré qu'un protocole d'échange d'information, qui n'a pas fait l'objet d'une publication officielle, ne pourrait pas être considéré comme constituant une dérogation à l'obligation d'information préalable.

En tenant compte de ce qui précède et s'agissant d'une matière réservée à la loi, la CNPD estime nécessaire d'encadrer la coopération des organismes publics dans le projet de loi, en indiquant les données susceptibles d'être échangées.

La CSSF et le CAA doivent encore informer la Caisse de consignation de toutes les sanctions administratives imposées, les recours et les résultats des recours (article 44, paragraphe 2, alinéa 2). Eu égard au libellé très vague de cette disposition et dans un souci de sécurité juridique et afin de respecter le principe de minimisation des données, le projet de loi devrait préciser quelles informations seraient, le cas échéant, transmises par la CSSF et le CAA à la Caisse de consignation.

ii. Accès au registre par l'Administration des contributions directes

Il ressort de l'article 38 de la loi en projet, que l'ACD peut accéder aux informations et documents conservés par la Caisse de consignation *« sous garantie d'un accès sécurisé, limité et contrôlé »*, afin d'accomplir ses missions prévues dans la loi du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) et de la loi modifiée du 24 juillet 2015 relative à FATCA. Il n'est pas précisé s'il s'agit d'un accès direct ou un accès sur demande.

Comme l'a soulevé le Conseil d'État dans son avis du 12 novembre 2017 relatif au projet de loi n°7182 *« étant donné que la communication de données informatiques à des tiers peut constituer une ingérence dans la vie privée et, partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle, il faut que le cadre légal contienne encore des dispositions pour garantir la sécurité de la transmission des données. »*[18].

[18] Avis n°52417 du Conseil d'État du 11 21 novembre 2017 relatif au projet de loi n°7182 portant modification
1) de la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'État ; 2) de la loi modifiée du 3 août 1998 instituant des régimes de pension spéciaux pour les fonctionnaires de l'État et des communes ainsi que pour les agents de la Société nationale des Chemins de Fer luxembourgeois ; 3) de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État ; 4) de la loi modifiée du 12 mai 2009 portant création d'une École de la 2e Chance ; 5) de la loi modifiée du 22 mai 2009 portant création a) d'un Institut national des langues ; b) de la fonction de professeur de langue luxembourgeoise ; 6) de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 7) de la loi modifiée du 25 mars 2015 instituant un régime de pension spécial transitoire pour les fonctionnaires de l'État et des communes ainsi que pour les agents de la Société nationale des Chemins de Fer luxembourgeois ; 8) de la loi modifiée du 25 mars 2015 fixant les conditions et modalités de l'accès du fonctionnaire à un groupe de traitement supérieur au sien et de l'employé de l'État à un groupe d'indemnité supérieur au sien ; 9) de la loi modifiée du 25 mars 2015 déterminant le régime et les indemnités des employés de l'État et portant abrogation de la loi modifiée du 22 juin 1963 portant fixation de la valeur numérique des traitements des fonctionnaires de l'État ainsi que des modalités de mise en vigueur de la loi du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État.

A l'instar dudit avis du Conseil d'État, la CNPD estime nécessaire d'insérer dans le libellé de l'article sous avis des dispositions analogues à celles contenues à l'article 138 de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration. Le libellé sous avis devra dès lors se lire comme suit :

« L'administration des contributions directes a droit, sur sa demande, aux données nécessaires pour la gestion des dossiers ouverts sur base de la loi du 18 décembre 2015 relative à la Norme commune de déclaration (NCD) et de la loi modifiée du 24 juillet 2015 relative à FATCA. Le système informatique par lequel sont transmises les données visées doit être aménagé de sorte que les informations relatives à la personne ayant procédé à la transmission, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation peuvent être retracés. »

III. Les droits des personnes concernées

Comme soulevé au point II.d. du présent avis, les articles 13 et 14 du RGPD imposent aux responsables du traitements une obligation d'information en cas de collecte directe (article 13) et collecte indirecte (article 14). Quant à la Caisse de consignation, le paragraphe 5 de l'article 14 du RGPD dispose, entre autre, que l'obligation d'information ne s'applique pas en cas de collecte indirecte, si l'obtention est prévue par le droit de l'Union ou le droit de l'État-membre et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée.

Afin d'assurer la protection des personnes physiques, la Commission nationale préconise que le responsable de traitement procède à une information claire et complète sur son site internet comportant les informations requises en vertu de l'article 14 du RGPD. Comme souligné par le GT29 dans ses lignes directrices sur la transparence, *« [u]n lien direct vers cette déclaration ou cet avis sur la protection de la vie privée devrait être clairement visible sur chaque page de ce site internet sous un terme communément utilisé (comme « Confidentialité », « Politique de confidentialité » ou « Avis de protection de la vie privée »).»*[19]

A titre d'information, la CNPD rappelle encore que l'exercice par les personnes concernées de leurs droits, tel que le droit d'accès, est gratuit pour les personnes concernées[20]. Par ailleurs, conformément à l'article 12, paragraphe 3 du RGPD, le responsable du traitement doit répondre la personne concernée dans le délai d'un mois à compter de la date de réception de la demande. Ce délai peut être prolongé de deux mois dans les conditions prévues au même paragraphe.

Il convient ainsi de souligner la différence entre le droit d'accès aux données à caractère personnel et la demande de restitution prévue à l'article 33 du projet de loi par laquelle *« toute personne justifiant d'un droit sur des avoirs consignés »* en vertu du projet de loi peut demander la restitution des avoirs. En effet, si une personne concernée exerce son droit d'accès auprès de la Caisse de consignation conformément à l'article 15 du RGPD, celle-ci doit

[19] Groupe de Travail « Article 29 », Lignes directrices sur la transparence au sens du règlement (UE) 2016/679, WP260 rev.01, p. 9.
[20] RGPD, article 12, paragraphe 5.

recevoir une réponse dans le délai d'un mois, si les conditions du RGPD sont remplies. Lorsqu'une personne dépose une demande de restitution conformément à l'article 33 du projet de loi, la Caisse de consignation devrait prendre une décision dans les six mois de la réception de la demande complète.

Ainsi décidé à Esch-sur-Alzette en date du 1er février 2019.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Commissaire	Christophe Buschmann Commissaire	Josiane Pauly Membre suppléant

ANNEXES

5

Avis de la Commission nationale pour la protection des données relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique.

Délibération n°36/2019 du 15 mars 2019

Conformément à l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après désignée « la directive »), à laquelle se réfère l'article 8 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données (ci-après désignée « loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD »), « conseille la Chambre des députés, le Gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données personnelles ».

Eu égard à la mission de conseil qui lui est attribuée, mais également de la tendance générale du renforcement de la surveillance des citoyens afin de pallier à l'insécurité et face aux préoccupations du public à ce sujet, la Commission nationale rend un avis circonstancié sur la création et l'exploitation par la Police grand-ducale d'un système de vidéosurveillance policière (ci-après désigné « VISUPOL ») au sein de zones de sécurités ciblées à Luxembourg-ville.

L'auto saisine de la CNPD intervient dans le cadre de l'abrogation de la base légale de VISUPOL suite à l'entrée en application de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. En effet, celle-ci abroge l'article 17 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, tel que modifié en 2007 (ci-après désignée « la loi du 2 août 2002 »). L'article en question fut le fondement légal de la création et de l'exploitation de VISUPOL. En application de l'article 17, un règlement grand-ducal du 1er août 2007 autorisait la création et l'exploitation de VISUPOL par la Police grand-ducale au sein de zones de sécurité (ci-après désigné « le règlement d'application »). Le règlement d'application déléguait la fixation des zones de sécurité concernées au ministre ayant dans ses attributions la Police grand-ducale à savoir, le Ministre de la Sécurité intérieure.

Les récentes modifications du cadre légal étant rappelées, la CNPD souhaite adopter une approche globale quant à l'utilisation de dispositifs de vidéosurveillance à des fins policières à savoir, la prévention, la recherche et la constatation des infractions[21]. Une telle approche nécessite de revenir sur les caractéristiques et les enjeux de la

[21] Conformément à l'article 17 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (abrogée) et l'article 2 de la loi du 18 juillet 2018 sur la Police grand-ducale et portant modification : 1° du Code de procédure pénale ; 2° de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État ; 3° de la loi du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 4° de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 5° de la loi du 18 décembre 2015 relative à l'accueil des demandeurs de protection internationale et de protection temporaire, et modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat ; et portant abrogation : 1° de la loi du 29 mai 1992 relative au Service de Police Judiciaire et modifiant 1. La loi du 23 juillet 1952 concernant l'organisation militaire ; 2. Le code d'instruction criminelle ; 3. La loi du 16 avril 1979 ayant pour objet la discipline dans la Force publique ; 2° de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

vidéosurveillance à des fins policières dans l'espace public (I), réflexion qui a pour objet de mettre en exergue l'importance de l'encadrement légal de la surveillance et du contrôle de l'espace public (II).

I. Les caractéristiques et les enjeux de la vidéosurveillance à des fins policières dans l'espace public

La vidéosurveillance policière, la captation d'images qui en émane et leurs utilisations ultérieures afin d'identifier les individus potentiellement dangereux ne sont pas de nouvelles méthodes. En effet, à la fin du XIX^{ème} siècle, le criminologue français Alphonse Bertillon, crée le premier laboratoire de police d'identification criminelle et l'anthropométrie judiciaire. Il développe des techniques de photographies uniformes et des méthodes de mesures du squelette humain afin d'identifier les criminels et les récidivistes[22].

De tous temps, les images du corps humains sont corrélées avec leurs comportements et présentées comme une solution miracle aux problèmes sociétaux[23]. Aujourd'hui encore, la vidéosurveillance est présentée comme le remède incontournable face à l'insécurité[24]. Néanmoins, les dispositifs de vidéosurveillance génèrent une surveillance et un contrôle social qu'il y a lieu de définir et d'analyser (A) afin de mesurer et de comprendre l'impact de tels dispositifs dans les droits et les libertés fondamentales reconnus aux individus (B).

A. Définir, comprendre, la surveillance et le contrôle social

Un cadre théorique qui s'imprègne de plusieurs disciplines telle que la sociologie et la philosophie, favorise la compréhension du fonctionnement de la surveillance et du contrôle mis en œuvre par un dispositif de vidéosurveillance policière tel que VISUPOL.

La sociologie tout d'abord, définit la surveillance comme étant « l'attention accrue portée à des personnes et des populations dans le but de les influencer, les gérer ou les contrôler »[25]. Les techniques de surveillance évoluent en fonction des évènements politiques, économiques et sociaux qui ponctuent et forgent la société. Le contrôle quant à lui, peut être défini comme l'action d'examiner ce qui est conforme ou ce qui ne l'est pas par rapport à une norme définie par le pouvoir. Il fait appel à la vérification du bon fonctionnement et de la qualité de la norme en question. La surveillance et le contrôle sont donc indissociables.

La philosophie quant à elle, favorise l'identification et la compréhension des caractéristiques de la surveillance et du contrôle. Michel Foucault dans son ouvrage *Surveiller et Punir. Naissance de la prison*[26] en identifie trois, à savoir : le découpage de l'espace (1), la surveillance hiérarchisée (2) et in fine, le savoir généré sur les individus (3).

1) Le découpage de l'espace

L'identification des zones urbaines à surveiller est caractéristique de toutes stratégies de surveillance et de contrôle.

[22] Pavlich, G, (2009), The subjects of criminal identification. Punishment & Society, 11 (2), p. 174 et suivantes. Voir également, Bertillon A., (1885), Identification anthropométrique. Instruction signalétique, Ministère de l'intérieur, Administration pénitentiaire, Melun, p. 132.
[23] Van der Walt J., (2015), « The Literary Exception : Reflections on Agamben's « Liberal Democratic » Political Theology and the Religious Destabilisation of the Political in our Time », in New perspectives. Interdisciplinary Journal of central & East European Politics and International Relations, 23 (1), p.17.
[24] Mucchielli L., Vous êtes filmés ! Malakoff, Armand Colin, p. 228.
[25] Lyon, D. « Le 11 septembre, la « guerre au terrorisme » et la surveillance généralisée », in Bigo, D., Bonelli, L., & Deltombe, T. (2008), Au nom du 11 septembre. Les démocraties à l'épreuve de l'antiterrorisme, Paris, La Découverte, p. 93.
[26] Foucault, M. (1975). Surveiller et Punir. Naissance de la prison. Editions Gallimard, p. 360.

Celle-ci y est généralement modulée en fonction des besoins de l'espace urbain et des risques qui y sont présents. A titre d'exemple, elle peut être plus intense dans une zone présentant un taux de criminalité élevé et peut être faible voire inexistante dans des quartiers résidentiels étant dénués de problèmes majeurs et n'ayant pas un degré d'activité élevé.

Les présentes considérations révèlent que la délimitation de ces zones se doit de répondre à des critères objectifs. A ce titre, le règlement d'application, pris en exécution de la loi du 2 août 2002, laquelle fût abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, nous renseigne sur les objectifs de VISUPOL et des zones de sécurité mises en place. Elles ont pour objet la prévention, la recherche et la constatation d'infractions pénales[27]. Il révèle également que le découpage de l'espace n'est pas permanent. En effet, l'article 10 paragraphe 2 du même règlement précise que les zones de sécurité à surveiller sont désignées comme telles pour une durée de deux ans. Une fois ce délai expiré, la vidéosurveillance peut être prorogée suite à une évaluation de l'utilité et de la nécessité de celle-ci.

Au regard des nombreux règlements ministériels rendus ces dernières années, la CNPD constate que la Police grand-ducale effectue un découpage de l'espace en désignant des zones de sécurité à Luxembourg-ville. A cet égard, le règlement ministériel du 15 septembre 2017 portant désignation des zones de sécurités soumises à la vidéosurveillance de la Police grand-ducale révèle quels sont les espaces découpés. Il s'agit du quartier du Limpertsberg-Glacis (Zone A), du quartier de la Gare (Zone C) ainsi que les environs du stade « Josy Barthel » (Zone D). Le règlement ministériel du 28 mars 2018 portant prorogation de la vidéosurveillance dans la zone de sécurité « zone E » à Luxembourg-ville[28] quant à lui, renseigne sur l'existence d'une zone de sécurité supplémentaire dans le quartier du Kirchberg, autour du Centre de Conférence.

2) Une surveillance hiérarchisée

Toute stratégie de surveillance et de contrôle obéit à une hiérarchie stricte favorisant l'organisation et la bonne mise en œuvre de celle-ci. Il y a ceux qui conçoivent et ordonnent la mise en œuvre d'une telle stratégie, ceux qui s'occupent de la gestion et d'autres qui l'exécutent. La loi du 18 juillet 2018 sur la Police grand-ducale, en particulier son Chapitre 2 Section 1ère consacrée aux missions de police administrative ne donne aucune précision quant à la hiérarchie qui orchestre et exécute la vidéosurveillance des quartiers de Luxembourg-ville précédemment mentionnés. Le Chapitre 4 de ladite loi relatif aux relations de la Police avec d'autres autorités fait certes état dans sa section 1ère, des relations entre la Police grand-ducale et les autorités communales, telles que les bourgmestres[29]. La composition et la mise en œuvre d'un comité de concertation régional[30] et d'un comité de prévention communal[31] y sont également mentionnés. Cependant, la CNPD constate qu'aucunes dispositions de ces articles ne sont consacrées aux acteurs impliqués dans le dispositif VISUPOL ne laissant pas entrevoir la hiérarchie qui orchestre ledit dispositif.

[27] Règlement grand-ducal du 1er août 2007 autorisant la création et l'exploitation par la Police d'un système de vidéosurveillance des zones de sécurité, Art. 1er.
[28] Ce règlement cessera d'être en vigueur le 28 mars 2019.
[29] Loi du 18 juillet 2018 sur la Police grand-ducale et portant modification: 1° du Code de procédure pénale ; 2° de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat ; 3° de la loi du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 4° de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 5° de la loi du 18 décembre 2015 relative à l'accueil des demandeurs de protection internationale et de protection temporaire, et modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat ; et portant abrogation : 1° de la loi du 29 mai 1992 relative au Service de Police Judiciaire et modifiant 1. La loi du 23 juillet 1952 concernant l'organisation militaire ; 2. Le code d'instruction criminelle ; 3. La loi du 16 avril 1979 ayant pour objet la discipline dans la Force publique ; 2° de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police, articles 35 et 36.
[30] Ibidem, article 37.
[31] Ibidem, article 38.

3) Générer un savoir sur les individus

Tout système de vidéosurveillance permet de générer un savoir conséquent sur les individus présents dans les zones de sécurité. L'attitude, la démarche, les activités et les déplacements des individus dans les lieux surveillés sont scrutés. Le regroupement de l'ensemble de ces éléments permet, dans une certaine mesure, de se faire une idée très précise sur les habitudes des individus surveillés et d'en générer un profil.

Cependant, la loi du 18 juillet 2018 sur la Police grand-ducale ne donne aucune indication relative au système VISUPOL si bien qu'il est impossible d'avoir des renseignements sur le type de savoir généré par le dispositif sur les individus. Des informations sont néanmoins données par l'article 3 du règlement d'application. Celui-ci dispose en effet que « le système de vidéosurveillance prend en image les zones de sécurité déterminées […] et enregistre ces images sur un outil informatique ». Il est donc possible d'en déduire que VISUPOL se limite à la captation d'image.

B. L'impact de la société de surveillance et du contrôle social sur les droits fondamentaux et les libertés reconnues aux individus

Les droits fondamentaux et les libertés reconnus aux individus bénéficient d'une protection considérable à l'échelle européenne. En effet, la Convention européenne des droits de l'Homme (ci-après désignée « la CEDH »), en est la première illustration.

De surcroît, le traité de Lisbonne renforce la garantie des droits fondamentaux en érigeant la Charte des droits fondamentaux (ci-après désignée « la Charte »), au rang du droit primaire de l'Union européenne[32]. L'article 2 du traité sur l'Union européenne dispose que cette dernière est fondée sur des valeurs telles que le respect de la liberté et des droits de l'hommes. Les juges de la Cour de justice de l'Union européenne (ci-après désignée « CJUE) ainsi que de la Cour européenne des droits de l'Homme[33] (ci-après désignée « Cour EDH »), se portent également garant du respect des droits fondamentaux et des libertés.

L'objet de la présente partie est de mettre en exergue l'impact que les systèmes de vidéosurveillance peuvent avoir sur les droits fondamentaux. Le recours aux dispositifs de surveillance peut avoir pour effet de limiter le respect au droit à la vie privée et à la protection des données (1), il peut également être générateur de discrimination et de stigmatisation (2) et limite le droit à la libre circulation des individus au sein de l'espace public (3)[34].

1) La limitation du droit à la vie privée et à la protection des données par les dispositifs de vidéosurveillance

La vidéosurveillance au sein de l'espace public a pour effet de limiter le droit à la protection des données à caractère personnel protégé par la Charte[35] et dans une plus large mesure, le droit au respect de la vie privée et familiale protégé à la fois par la Charte[36] et la Convention européenne des droits de l'Homme[37] mais également

[32] Article 6 paragraphe 1 du traité sur l'Union européenne, J.O.U.E., C 326, 26.10.2012, p. 13-390.
[33] La CNPD se focalisera davantage sur les arrêts rendus par la CJUE mais ce n'est pas pour autant qu'elle ignore les jugements rendus par la CEDH.
[34] La CNPD limite son analyse à ces trois droits fondamentaux mais cela ne veut pas dire que l'impact de la vidéosurveillance est limité à ces derniers.
[35] Article 8 de la Charte des droits fondamentaux de l'Union européenne, J.O.C.E., C 326 du 26.10.2012, p. 391.
[36] *Ibidem.*
[37] Article 8 de la Convention européenne des droits de l'Homme, signée à Rome, le 4.XI.1950.

par la Constitution Luxembourgeoise[38]. En effet, de tels dispositifs génèrent un savoir sur les individus, savoir qui a notamment fait l'objet de développements dans la jurisprudence de la CJUE et la Cour EDH.

A titre liminaire, la Commission nationale rappelle les propos de l'avocat général Villalon dans le cadre de l'arrêt de la CJUE *Digital Rights* qui affirme que ce savoir génère une « cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire un portrait complet et précis de son identité privée »[39]. La CNPD peut s'inspirer de cet arrêt de la CJUE et observer que les images émanant des dispositifs de vidéosurveillance « prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci »[40].

La Cour européenne des droits de l'homme quant à elle, considère également que le fait de surveiller les actes de personnes se trouvant dans un lieu public, notamment au moyen d'un système de vidéosurveillance, entraîne une ingérence dans la vie privée de ces personnes si le fait de surveiller est accompagnée d'un enregistrement et se fait de manière systématique ou permanente.[41]

La vidéosurveillance peut également avoir pour effet de générer de la discrimination et de la stigmatisation des individus se trouvant au sein des zones de sécurité.

2) La vidéosurveillance génératrice de discrimination et de stigmatisation

L'Union européenne est fondée sur des valeurs dont la non-discrimination fait partie[42]. L'interdiction de discrimination est également consacrée par la CEDH[43], la Charte[44] ainsi qu'au sein de la Constitution Luxembourgeoise[45].

A ce titre, la Commission nationale souhaite rappeler que les individus ne sont pas tous égaux face à la vidéosurveillance. En effet, le grand nombre de personnes se trouvant dans les zones surveillées et l'incalculable quantité d'images collectées sont autant de facteurs qui compliquent l'observation policière. Pour mener à bien sa mission, la police se doit donc d'effectuer une sélection des personnes à surveiller et des images collectées. Une distinction de ceux qui ont un comportement suspect et ceux qui en sont dénués s'opère.

De telles pratiques amènent la CNPD à s'interroger sur ce qu'est un comportement suspect et quels sont les critères permettant à la police d'identifier de tels comportements ?

Dans leur étude relative à l'impact de la vidéosurveillance, Prof. Norris et Prof. Armstrong révèlent que l'appartenance sociale, l'âge, l'ethnicité et le genre peuvent être des critères de sélection pris en compte par la police afin de cibler davantage l'observation des individus[46]. La démarche des individus, leurs styles vestimentaires, s'ils sont actifs, passifs, provoquants etc.,[47] sont autant d'éléments pris en compte lors de la surveillance. Leur étude révèle également que 36% des personnes sujettes à une étroite observation le sont pour des « raisons évidentes », 24% des

[38] Article 11 (3), Constitution, Texte Coordonné à jour au 20 octobre 2016, Recueil réalisé par le Ministère d'État – Service central de législation.
[39] Conclusion de l'avocat général Pedro Cruz Villalon dans les affaires jointes Digital Rights Ireland Seitlinger e.a., C-293/12 et C-594/12, EU :C :2013 :845, point 74.
[40] Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :201 :2014 :238, point 27.
[41] Cour EHD, Peck c. Royaume-Uni, n°44647/98, 28 janvier 2003, para.59.
[42] Traité sur l'Union européenne, J.O.U.E., C326, 26.10.2012, p. 13-390, article 2.
[43] Article 14.
[44] Article 21.
[45] Article 10 bis.
[46] Norris, C. and Armstrong, G., The Maximum, Surveillance Society: The Rise of CCTV, (1999 b), Oxford:Berg. Etude reprise in Lyon, D., Surveillance as social sorting. Privacy, risk and digital discrimination, Routledge, (2008), p. 266.
[47] *Ibidem.*

personnes sont surveillées à cause de leurs comportements et 34% sur base de leur appartenance ethnique. Autres chiffres révélateurs : 65% des adolescents sont surveillés sans motifs particuliers, 68 % personnes de couleur ont fait l'objet d'une observation ciblée également sans motifs. Par conséquent, les jeunes, les personnes de couleurs et les hommes sont les personnes les plus surveillées sans motifs[48]. Ils concluent qu'une telle différenciation n'est pas basée sur des critères comportementaux et individuels objectifs mais fondée sur l'appartenance à un groupe social et par conséquent, ces pratiques sont discriminatoires pouvant accentuer la marginalisation et la stigmatisation des personnes ciblées[49] aboutissant à la mise en œuvre d'un tri social[50].

L'installation et l'utilisation de vidéosurveillance peut également avoir pour effet de limiter le droit à la libre circulation.

3) La limitation du droit à la libre circulation

La libre circulation des personnes est un droit fondamental de l'Union européenne. Il est consacré à l'article 2 du Protocole additionnel n°4 à la CEDH ainsi qu'à l'article 45 de la Charte des droits fondamentaux de l'Union européenne.

Il est indéniable que l'utilisation de vidéosurveillance dans les lieux publics limite la portée du droit à la libre circulation. En effet, les images émises par les dispositifs de vidéosurveillance peuvent avoir pour effet de suivre les individus, tracer leurs itinéraires quotidiens. Les individus peuvent avoir l'impression de ne pas être en mesure de circuler librement dans l'espace public sans faire l'objet d'un suivi constant[51].

L'étude des caractéristiques, des enjeux de la vidéosurveillance à des fins policières dans l'espace public étant faite et la nécessaire prise en considération du cadre légal actuellement en vigueur étant rappelée, il y a à présent lieu de souligner l'importance de l'encadrement légal de la surveillance et du contrôle qui prennent place au sein de l'espace public.

II. L'importance de l'encadrement légal de la surveillance et du contrôle de l'espace public

Doter d'une base légale un système de vidéosurveillance policière mis en œuvre au sein de l'espace public permet de poser des garde-fous quant à son utilisation et établir des garanties pour les personnes qui sont sujettes à la surveillance et au contrôle qui en émane. L'encadrement par un texte de loi d'un tel dispositif permet de freiner l'ubiquité de son installation et de ne pas considérer l'ensemble des individus comme des suspects potentiels.

L'objet de la présente partie est de mettre en exergue la manière dont le droit européen circonscrit l'ingérence faite dans les droits fondamentaux par des dispositifs de surveillance (A) et façonne le droit national en la matière (B).

A. L'encadrement de l'ingérence dans les droits fondamentaux occasionnées par des dispositifs de surveillance par le droit européen

[48] *Ibidem.*
[49] *Ibidem.*
[50] Lyon D. (2003). Surveillance as a social sorting: Privacy, risk, and digital discrimination. Psychology Press, p.20.
[51] Groupe de travail « Article 29 » sur la protection des données, Avis 4/2004 sur le traitement des données à caractère personnel au moyen de la vidéo-surveillance, adopté le 11 février 2004, 117/02/FR WP 89, disponible à la page : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp089_fr.pdf, consultée pour la dernière fois le 14/02/2019.

ANNEXES

5

L'impératif d'une base légale (1) et la qualité de la loi (2) sont des critères consacrés par le droit européen afin d'encadrer l'ingérence dans les droits fondamentaux émanent de stratégies de surveillance.

1) L'impératif de la base légale

La CNPD souhaite rappeler que le respect des droits fondamentaux n'est pas absolu puisqu'une ingérence dans ces derniers est reconnue à l'article 52 paragraphe 1 de la Charte. En effet, cet article dispose que « toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi »[52]. La CEDH quant à elle, rend également possible ladite limitation tout en la rattachant au respect de la vie privée et familiale par exemple[53].

La CJUE et la Cour EDH se sont prononcées à de nombreuses reprises sur la nécessité d'une loi encadrant l'atteinte qui est faite dans les droits fondamentaux. Dans l'arrêt *Digital Rights*[54] relatif à l'appréciation de la validité de la directive 2006/24/CE avec les articles 7 et 8 de la Charte ou encore dans l'avis 1/15 relatif à la conclusion de l'accord Passenger Name Record (PNR) entre l'Union européenne et le Canada[55], la CJUE a eu l'occasion de rappeler l'obligation de prévoir légalement toute ingérence dans les droits fondamentaux. La Cour EDH dans son arrêt *Kopp*[56] relatif à la mise sur écoute des lignes téléphoniques d'un cabinet d'avocats sur instruction du procureur général de la Confédération helvétique ainsi que dans l'arrêt *Amann*[57] relatif à l'interception d'une communication téléphonique, procède à la vérification de l'existence d'une base légale justifiant les limitations dans les droits fondamentaux, en particulier le droit au respect de la vie privée et familiale.

Emane de l'impératif que l'ingérence soit prévue par la loi, l'exigence de la qualité de celle-ci.

2) La qualité de la loi

La qualité de la loi, en particulier en matière pénale, s'apprécie au regard du respect du principe de légalité des incriminations. En effet, la légalité des peines est l'énonciation dans la loi des comportements incriminés[58]. Elle a pour effet d' « assurer la meilleure connaissance possible de la loi pénale ; favoriser la prévisibilité et sécurité dans les échanges sociaux[59] », garantir le principe de la hiérarchie ; de séparation des pouvoirs et par là, limiter l'arbitraire du juge. A l'échelle supra nationale, ce principe est consacré par la CEDH à son article 7 qui le perçoit comme un droit absolu auquel nul ne peut déroger[60]. Par conséquent, celui-ci appartient aux principes généraux du droit de l'Union européenne[61].

Du principe de légalité émane la prévisibilité de la loi, principe selon lequel un individu suffisamment informé doit savoir quels sont les comportements pouvant faire l'objet d'une surveillance dans l'espace public.

[52] *J.O.U.E.*, C 326, 26.10.2012, p.391-407.
[53] Article 8 paragraphe 2 de la Convention européenne des droits de l'Homme, signée à Rome, le 4.XI.1950.
[54] Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :201 :2014 :238, point 38.
[55] Avis 1/15, du 8 septembre 2016, EU :C :2016 :656.
[56] Cour EDH, Kopp c. Suisse, n°23224/94, 25 mars 1998, para. 56 à 61.
[57] Cour EDH, Amann c. Suisse [GC], n°27798/95, 16 février 2000, para. 46 à 54.
[58] Beccaria, C., (1870). Des délits et des peines. Guillaumin.
[59] Carluyvels Y., « Les paradigmes du droit penal moderne en période « postmoderne »: évolutions et transformations, *in* Massé M., J-P. Jean, Giudicelli A. (sous la dir), (2009). Un droit pénal postmoderne ? Mise en perspective des évolutions et ruptures contemporaines. Presses universitaires de France, p. 77.
[60] Carluyvels Y., Guillain C., Kerchove M., Tulkens F. (Ed.), (2010), *Introduction au droit pénal. Aspects juridiques et criminologiques,* Bruxelles, Kluwer, p. 225.
[61] Traité sur l'Union européenne, J.O.U.E., C 326, 26.10.2012, p. 13-390, article 6 paragraphe 3.

Ainsi, conformément au principe de légalité de la loi pénale, la CNPD affirme que les individus doivent pouvoir être tenus informés sur les comportements qui attirent particulièrement l'attention des agents de la Police grand-ducale lors de visionnage des images.

La Cour EDH et la CJUE rappellent également quels sont les critères que la loi doit remplir pour faire preuve de qualité.

La Cour EDH affirme que les mots « prévue par la loi » impliquent des conditions qui vont au-delà de l'existence d'une base légale en droit interne et exigent que celle-ci soit « accessible » et « prévisible » »[62]. Elle ajoute que ces termes impliquent que « le droit interne doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par l'article 8 paragraphe 1 »[63]. Par conséquent, la loi « doit définir l'étendue et les modalités d'exercice du pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire »[64].

La CJUE quant à elle, rappelle l'importance « de prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »[65].

L'encadrement de l'ingérence dans les droits fondamentaux et les libertés étant effectué par le droit européen, il y a à présent lieu d'analyser la mise en œuvre d'un tel encadrement à l'échelle nationale.

B. La limitation de l'exercice des droits fondamentaux par le droit national

Compte tenu de l'obligation imposée par le droit européen et au regard de la jurisprudence de la CJUE et la Cour EDH, la CNPD estime qu'en principe, les États-membres n'ont pas d'autres choix que de prévoir une base légale pour toute limitation à l'exercice des droits fondamentaux et des libertés. L'installation de systèmes de vidéosurveillance à des fins policières ne fait pas exception à la règle. De nombreux pays européens ayant recours à la vidéosurveillance dans l'espace public dote cette dernière de base légale, c'est le cas de nos pays voisins, la France (1), la Belgique (2) et l'Allemagne (3).

1) L'exemple français

En France, le nombre de caméras filmant l'espace public a fortement augmenté pour lutter contre l'insécurité[66]. L'installation de systèmes dits de vidéo protection est prévue par le Code de la sécurité intérieure[67]. Les objectifs de l'installation de tels dispositifs au sein de l'espace public y sont prévus. Il s'agit notamment de prévenir les atteintes à la sécurité des personnes et des biens dans des zones déterminées[68], de prévenir des actes de terrorisme[69],

[62] Cour EDH, Amann c. Suisse [GC], n°27798/95, 16 février 2000, para, 55.
[63] *Ibidem,* para 56.
[64] *Ibidem.* Voir également Cour EDH, Malone c. Royaume-Uni, série A n°82, du 2 août 1984, pp. 31-32, para.66 ; Cour EDH, Fernández Martínez c. Espagne CE:ECHR:2014:0612JUD005603007, 12 juin 2014 para.117 ; Cour EDH, Liberty et autres c. Royaume-Uni, n°58243/00, du 1er juillet 2008, para. 62 et 63; Cour EDH, Rotaru c. Roumanie, App. N°28341/95, 4 mai 2000, para. 57 à 59 et Cour EDH, S et Marper c. Royaume-Uni, Requêtes n°30562/04 et 30566/04, du 4 décembre 2008 para. 99.
[65] Arrêt du 6 octobre 2015, Schrems, C-362/14, EU :C :2015 :650, point 91. Voir également en ce sens Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :201 :2014 :238, point, 54,
[66] Mucchielli L., *Vous êtes filmés !* Malakoff, Armand Colin, p. 25 et suivantes.
[67] Titre V du Code de la sécurité intérieure.
[68] *Ibidem,* article L251-2, 5°.
[69] *Ibidem,* articles L251-2, 6° et articles L223-1 et suivants.

des risques naturels ou technologiques etc.[70]. En ce qui concerne leurs autorisations, celles-ci sont données par le préfet[71] pour une durée de cinq ans renouvelable[72]. Le Code de la sécurité intérieure fait également mention des personnes en charge du visionnage des images[73], celles et ceux pouvant avoir accès à ces dernières[74] ainsi que la durée de conservation des images qui ne peut excéder un mois[75]. De surcroit, les autorités en charge de la gestion et de l'évaluation des dispositifs de vidéo protection telles que les Commissions départementales[76] et nationale[77] de la vidéo protection et la Commission nationale de l'informatique et des libertés[78] y sont également précisées.

Le présent développement révèle que la France a doté d'une base légale l'installation et la mise en œuvre des caméras de surveillance au sein de l'espace public. Celle-ci répond aux critères de qualité de la loi consacrés par le droit européen et la jurisprudence de la Cour EDH et de la CJUE.

2) L'exemple belge

En Belgique, la loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police[79] est la base légale encadrant la vidéosurveillance dans l'espace public à des fins policières. Cette loi intervient dans un contexte de lutte anti-terroriste et anticipe l'entrée en application du RGPD et de la directive. Celle-ci prévoit en effet les conditions dans lesquelles les services de police peuvent avoir recours au dispositif de vidéosurveillance[80]. La loi précise également que l'utilisation d'un tel dispositif s'effectue sur décision et sous la responsabilité du fonctionnaire de police qui est également tenu de veiller au respect des principes de proportionnalité et de subsidiarité[81]. Tout comme la loi française, la législation belge prévoit une autorité en charge de l'évaluation des dispositifs de vidéosurveillance. En effet, il s'agit du Conseil Communal de la commune concernée par l'installation de ces derniers ou du ministre de l'Intérieur (ou de son délégué), concernant les services de police fédérale[82].

De surcroît, la durée de conservation n'excédant pas douze mois des données à caractère personnel collectées par les caméras[83], ainsi que l'accès aux images pour des finalités judiciaires et autres, sont prévus[84].

Il ressort du présent développement que les dispositifs de vidéosurveillance au sein de l'espace public à des fins policières est prévu légalement en droit belge. Il en est de même en droit allemand.

3) L'exemple allemand

La loi fondamentale pour la République fédérale d'Allemagne protège entre autres, la dignité de l'être humain et le caractère obligatoire des droits fondamentaux pour la puissance publique[85], la liberté d'agir, l'égalité devant la loi[86] ou encore la liberté de circulation et d'établissement[87]. De surcroît, la loi fondamentale prévoit que la restriction d'un droit fondamental doit être prévu par la loi[88].

[70] *Ibidem,* article L251-2.
[71] *Ibidem,* article L252-1.
[72] *Ibidem,* article L252-2
[73] *Ibidem,* article L252-2.
[74] *Ibidem,* article L252-3.
[75] *Ibidem,* article L252-5.
[76] *Ibidem,* articles L251-4 ; L253-1.
[77] *Ibidem,* articles L251-5, 6 et 7.
[78] *Ibidem,* articles L251- 4 et ; L253-2, 3, 4 et 5.
[79] modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière.
[80] *Ibidem,* article 8.
[81] *Ibidem,* article 10.
[82] *Ibidem,* article 9.1.
[83] *Ibidem,* article 11.
[84] Ibidem, article 12.
[85] Deutscher Bundestag, Loi fondamentale pour la République fédérale d'Allemagne, article 1, La loi est disponible à l'adresse : https://www.bundestag.de/resource/blob/189762/f0568757877611b2e434039d29a1a822/loi_fondamentale-data.pdf, consultée pour la dernière fois le 14/03/2019.
[86] *Ibidem,* article 18.
[87] *Ibidem,* article 11.
[88] *Ibidem,* article 19.

La Cour constitutionnelle allemande veille au respect de l'article 19 de la loi fondamentale puisqu'elle consacre l'exigence d'une base légale pour la vidéosurveillance des espaces publics. Elle s'est aussi préoccupée de la surveillance des comportements des personnes concernées qui représente selon elle une atteinte aux droits fondamentaux. Le caractère attentatoire aux droits fondamentaux ne disparaît ni par le fait que la vidéosurveillance ait lieu dans l'espace public (et non en des lieux privés), ni par l'information des personnes concernées, ni par l'absence de contestations de la part de celles-ci[89]. La Cour constitutionnelle en déduit que la mise en place d'une vidéosurveillance nécessite une base légale qui doit respecter les principes de clarté et proportionnalité.[90] L'absence d'une telle législation a pour conséquence de soumettre les citoyens à l'arbitraire des autorités[91]. La Cour précise également que le degré de précision de la loi requis est déterminé en fonction de l'intensité de l'atteinte aux droits fondamentaux, et, pour ce qui est de la vidéosurveillance d'un lieu public, l'atteinte est jugée particulièrement importante puisqu'il s'agit d'une mesure visant indistinctement toutes les personnes se trouvant sur les lieux faisant l'objet d'une vidéosurveillance et que la plupart des personnes concernées n'ont rien à se reprocher[92].

C'est aux Länder que revient la responsabilité de légiférer en matière de vidéosurveillance au sein de l'espace public. A ce titre, la Rhénanie-du-Nord-Westphalie[93] et Hambourg[94] peuvent être pris pour exemple[95]. Ces législations déterminent les critères en fonction desquels les caméras sont installées, les personnes et institutions décidant de la mise en place des caméras et la durée de conservation des images.

Pour ce qui est des critères déterminant les lieux d'installation des caméras, il y a lieu, selon ces législations, de tenir compte des infractions ayant été commises dans le passé et ce celles probables dans le futur.

La législation du Land de Rhénanie-du-Nord-Westphalie précise par ailleurs que la vidéosurveillance ne peut être mise en œuvre que s'il est assuré que la Police peut intervenir très rapidement en cas d'infraction. En effet, une vidéosurveillance d'un côté sans garantie d'une intervention rapide de l'autre est jugée inadmissible pour l'État de droit.[96]

Ainsi, tout comme ses voisins français et belge, l'Allemagne encadre légalement l'installation et la mise en œuvre de la vidéosurveillance au sein de l'espace public et respecte le droit européen et la jurisprudence des juridictions européennes à cet égard.

Conclusion

L'étude des caractéristiques et des enjeux de la vidéosurveillance à des fins policières dans l'espace public, la surveillance, le contrôle social qui en émanent et l'impact de tels dispositifs dans les droits fondamentaux et les libertés reconnues aux individus, sont autant de raisons qui justifient l'importance de l'encadrement légal des dispositifs tels que VISUPOL.

[89] Bundesverfassungsgericht, Beschluss vom 23. Februar 2007 - 1 BvR 2368/06, points 38 à 40, disponible à la page : https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2007/02/rk20070223_1bvr236806.html, consultée pour la dernière fois le 13/03/2019.
[90] *Ibidem,* point 41.
[91] *Ibidem,* point 46.
[92] *Ibidem,* points 51 et 52.
[93] § 15a Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW), disponible à la page: https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=1&bes_id=5173&anw_nr=2&aufgehoben=N&det_id=423939, consultée pour la dernière fois le 13/03/2019.
[94] § 8 Abs. 3 PolDVG (Gesetz über die Datenverarbeitung der Polizei), disponible à la page: http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&doc.id=jlr-PolDVGHArahmen&doc.part=X&doc.origin=bs, consultée pour la dernière fois le 13/03/2019.
[96] Voir à ce sujet les travaux parlementaires de la législation du Land de Rhénanie-du-Nord-Westphalie p.10 disponibles à la page : https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMD17-3865.pdf,consultée pour la dernière fois le 13/03/2019.

En effet, la CNPD constate que comme tout dispositif de vidéosurveillance, VISUPOL est un instrument qui génère une surveillance permanente et un contrôle des individus. Par conséquent, ce dispositif de surveillance policière effectue une ingérence dans le droit à la vie privée et à la protection des données. Il est également susceptible d'entraver le droit à la non-discrimination et de limiter la libre circulation des personnes au sein de l'espace public.

Néanmoins, la Commission nationale souhaite rappeler que de telles limitations sont possibles à condition d'être légalement prévues. L'existence d'un tel impératif s'explique notamment par le fait que les personnes dont les droits fondamentaux et les libertés sont limités doivent disposer de garanties suffisantes permettant de se protéger efficacement contre les risques d'abus à leur encontre[97].

La base légale est également utile aux législateurs et aux juges dans l'appréciation de la nécessité et du caractère proportionné de la mesure qui sont des conditions parmi d'autres que les ingérences doivent remplir[98]. Par conséquent, elle permet de s'assurer que l'installation et l'utilisation de la vidéosurveillance à des fins policières répond à des critères objectifs tel que la lutte contre la délinquance et non subjectifs tel que le sentiment d'insécurité ressenti par les individus.

Ainsi, compte tenu de l'abrogation de la loi de 2002 et des règlements grand-ducaux sur lesquels le dispositif VISUPOL repose et les termes généraux dont fait preuve la loi relative aux missions de la Police grand-ducale, la CNPD suggère que les dispositions légales de cette dernière soient davantage précisées afin d'inclure VISUPOL dans son champ d'application.

Toutefois, la CNPD se demande s'il ne serait pas plus opportun que le Luxembourg se dote d'une loi spécifique encadrant l'installation et l'exploitation de dispositif de vidéosurveillance dans l'espace public à des fins policières comme le font la France, la Belgique et l'Allemagne.

Dans ce contexte, la CNPD salue la déclaration récente du Ministre de la Sécurité intérieure qui considère *« qu'il est opportun de réfléchir à la mise en place d'un cadre légal spécifique pour l'installation future de caméras de surveillance »*[99]. Cette prise de position concorde d'ailleurs avec la volonté du gouvernement de vouloir légiférer pour ce qui est de l'utilisation projetée des « bodycams » par la Police grand-ducale si l'on se réfère à l'accord de coalition du gouvernement qui précise que : *« L'expérience pratique visant l'introduction des caméras portées sur le corps et, le cas échéant, de caméras embarquées dans les véhicules sera menée. Un cadre légal précis et applicable en matière d'enregistrement des données à caractère personnel lors des interventions policières devra être établi »*. Les présentes suggestions de la Commission nationale se font également l'écho des principes de légalité et de qualité de la loi, consacrés par le droit européen et la jurisprudence de la Cour de Justice de l'Union Européenne et la Cour Européenne des Droits de l'Homme.

[97] *Ibidem,* point 54.
[98] Article 52 paragraphe 1 de la Charte des droits fondamentaux d l'Union européenne, J.O.U.E., C 326, 26.10.2012, p.391-407.
[99] Communiqué par le ministère de la Sécurité intérieure du 12/03/2019, disponible à la page : https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2019/03-mars/12-bausch-videoprotection.html, consultée pour la dernière fois le 12/03/2019.

La CNPD souhaite ajouter que le présent avis n'est pas limité au dispositif VISUPOL de la Police grand-ducale qui, pour l'instant n'est opérée que sur le seul territoire de la Ville de Luxembourg. En effet, dans la mesure où les responsables de certaines communes ont aussi manifesté leur intention de vouloir surveiller des espaces et lieux publics situés sur leurs territoires communaux, le présent avis a une portée générale qui a vocation à couvrir tout dispositif de vidéosurveillance, ayant une finalité de sécurité publique, peu importe qu'il soit opéré au niveau national par la Police grand-ducale ou au niveau local par des communes.

Ainsi, quel que soit le choix de base légale, celle-ci aura pour effet de mettre en exergue qu'au sein d'une démocratie telle que le Luxembourg, un des pays fondateurs de l'Union européenne et protecteurs de ses valeurs[100], la Police grand-ducale ou encore les communes, exercent leurs missions de surveillance résultant d'une interaction complexe entre des règles juridiques, organisationnelles, professionnelles, situationnelles et interactionnelles[101].

Ainsi décidé à Esch-sur-Alzette en date du 15 mars 2019.

La Commission nationale pour la protection des données

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann
Présidente	Commissaire	Commissaire

[100] Article 2 du Traité sur l'Union européenne,
[101] Lyon D., Surveillance as social sorting: Privacy, risk, and digital discrimination, Routledge, 2003, p.252

ANNEXES

5

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7373 concernant la limitation de la portée de certains droits et obligations dans le cadre du règlement général sur la protection des données et portant : 1. mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ; 2. modification de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et 3. modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances.

Délibération n°38/2019 du 5 avril 2019

Conformément à l'article 57, paragraphe 1er, lettre (c) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

Faisant suite à la demande lui adressée par Monsieur le Ministre des Finances en date du 18 octobre 2018, la Commission nationale entend présenter ci-après ses réflexions et commentaires relatifs au projet de loi n°7373 concernant la limitation de la portée de certains droits et obligations dans le cadre du règlement général sur la protection des données et portant : 1. mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ; 2. modification de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; et 3. modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances (ci-après « le projet de loi »).

Selon l'exposé des motifs, ce projet de loi entend modifier la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier (ci-après « la loi modifiée du 23 décembre 1998 ») et

la loi modifiée du 7 décembre 2015 sur le secteur des assurances (ci-après « la loi modifiée du 7 décembre 2015 ») afin de permettre à la Commission de surveillance du secteur financier (ci-après « la CSSF ») et au Commissariat aux Assurances (ci-après « le CAA ») de se prévaloir de certaines des limitations énoncées à l'article 23, paragraphe 2 du RGPD dans l'accomplissement de leurs missions.

Le RGPD, qui est d'application directe dans tous les États-membres de l'Union européenne depuis le 25 mai 2018, entend protéger les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel (article 1er, paragraphe 2). Il vise à harmoniser les règles européennes existantes afin *« d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union »*[102] et à moderniser la directive 1995/46/CE (transposée en droit luxembourgeois par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel) dans une société de plus en plus digitale en redonnant aux citoyens le contrôle des données qui les concernent, que celles-ci soient collectées et utilisées par les acteurs économiques privés ou par les acteurs du service public[103].

Le RGPD confère en particulier dans son chapitre III (articles 12 à 23) différents droits aux personnes concernées, leur permettant de contrôler l'usage des données à caractère personnel les concernant. Son article 23 prévoit cependant que le droit d'un État-membre peut, par la voie de mesures législatives, limiter la portée de ces droits, 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 un des objectifs prévus limitativement à l'article 23, paragraphe 1er, à condition que cette mesure législative prévoit des dispositions spécifiques relatives au moins aux éléments visés à l'article 23, paragraphe 2. Par ailleurs, les limitations doivent respecter les exigences énoncées par la Charte des droits fondamentaux de l'Union européenne (ci-après « la Charte ») et par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après « la Convention »)[104].

La Commission nationale a déjà eu l'occasion de se prononcer sur les clauses d'ouverture de l'article 23 du RGPD dans le cadre de son avis du 29 mars 2018 relatif au projet de loi n°7250 portant exécution, en matière fiscale, des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE et portant modification de dispositions diverses (délibération n°219/2018), dans lequel elle a fourni des précisions quant aux modalités de mise en œuvre des clauses d'ouverture et des garanties, qui doivent être intégrées dans la mesure législative pour assurer le respect du RGPD.

Ayant déjà été consultée par le ministère des Finances au stade d'avant-projet de loi en question, la Commission nationale se limite à formuler les observations suivantes.

[102] Cf. RGPD, considérant 10.

[103] Pour plus d'informations à ce sujet, voir l'avis de la Commission nationale pour la protection des données du 28 décembre 2017 relatif au projet de loi portant création de la Commission nationale pour la protection des données et la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, document parlementaire 7184/3.

[104] Cf. RGPD, considérant 73.

ANNEXES

5

I. Considérations générales

Les auteurs du projet de loi ont souhaité prévoir dans un article de chacune des lois modifiées, à savoir le nouvel article 16-3 de la loi modifiée du 23 décembre 1998 et le nouvel article 13-3 de la loi modifiée du 7 décembre 2015, les cas de figure (listés sous les lettres (a) à (f)) permettant à la CSSF et au CAA de limiter le droit à l'information des personnes concernées lorsque les données à caractère personnel sont collectées auprès de celles-ci, tel que prévu à l'article 13 du RGPD. Les nouveaux articles 16-4 à 16-7 de la première loi citée, de même que les nouveaux articles 13-4 à 13-7 de la seconde, introduisent quant à eux des limitations à d'autres droits des personnes concernées consacrés par le RGPD, à savoir le droit à l'information des personnes concernées lorsque les données à caractère personnel n'ont pas été collectées auprès de celles-ci (article 14 du RGPD), le droit d'accès (article 15 du RGPD), le droit à la limitation du traitement (article 18 du RGPD), et le droit d'opposition (article 21 du RGPD). Chacune de ces dispositions renvoie aux cas de figure décrits aux lettres (a) à (f) de l'article 16-3 de la première loi ou 13-3 de la seconde.

Or, la CNPD constate que seul le commentaire des articles 16-3 de la loi modifiée du 23 décembre 1998 et 13-3 de la loi modifiée du 7 décembre 2015 explique de manière exhaustive la nécessité de chacun de ces cas de figure, visés aux lettres (a) à (f) desdits articles, dans lesquelles le droit à l'information pourrait être limité par la CSSF ou par le CAA. Les commentaires des articles 16-4 à 16-7 de la première loi citée, et des articles 13-4 à 13-7 de la seconde, se contentent quant à eux de décrire de manière générale la nécessité de limiter les autres droits du RGPD, sans pour autant fournir des explications spécifiques démontrant la nécessité des différents cas de figure dans lesquelles chacun de ces droits pourrait être limité.

La CNPD regrette que la nécessité et la pertinence des différents cas de figure associés à chacun des droits des personnes concernées n'ait pas été davantage expliqué dans le commentaire des articles.

Par exemple, les lettres (f) des articles 16-3 de la loi modifiée du 23 décembre 1998 et 13-3 de la loi modifiée du 7 décembre 2015 prévoient que la CSSF ou le CAA pourraient limiter le droit à l'information, si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF ou du CAA *« porte atteinte à des intérêts légitimes protégés de tiers »*. Selon le commentaire des articles, cette exception pourrait notamment être importante dans le cadre de l'article 15 du RGPD, à savoir le droit d'accès, par exemple pour protéger les intérêt d'un tiers, qui a révélé des informations sensibles à la CSSF (tel qu'un lanceur d'alerte)[105]. Or, la disposition en question concerne l'article 13 et non pas l'article 15 du RGPD. Ce dernier dispose d'ores et déjà que le droit d'obtenir une copie ne doit pas porter préjudice aux droits et libertés d'autrui.

Par ailleurs, pour ce qui est de la lettre (b) des mêmes articles, la CNPD comprend du commentaire des articles que les auteurs du projet de loi visent principalement le droit à l'information des personnes concernées et le droit d'accès dans des cas très précis, principalement justifiés par *« l'impact d'une communication de certaines*

[105] Projet de loi n°7373, doc. parl. 7373/00, p. 18.

informations à la personne concernée sur le bon fonctionnement des marchés ou la stabilité financière, voire la sécurité publique et l'ordre public en cas de crise importante, si une telle information est concrètement de nature à créer ce risque (par exemple un « bank run ») »[106]. Alors qu'elle comprend cette justification, la CNPD suggère de limiter ce cas de figure aux articles 16-3 à 16-5 de la loi modifiée du 23 décembre 1998 et 13-3 à 13-5 de la loi modifiée du 7 décembre 2015, alors qu'ils ne visent ni le droit à la limitation du traitement ni le droit d'opposition. Elle recommande par ailleurs de justifier ces cas de figure dans le corps même du texte du projet de loi, afin de circonscrire la portée de cette limitation.

Enfin, la CNPD suggère de remplacer la formulation « l'intérêt privé » employée aux lettres (a) et (b) des mêmes articles par la formulation « les intérêts ou les droits et les libertés de celle-ci » et de rajouter « public » entre « l'intérêt » et « poursuivi par la CSSF », afin d'aligner la terminologie de projet de loi sur la terminologie employée par le RGPD.

II. <u>Les données traitées par la CSSF (article 16-1 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-1 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi)</u>

Selon le commentaire des articles, les données qui sont traitées sont *« essentiellement les indications visées sur les papiers d'identités de la personne concernée, les données normalement inscrites sur un curriculum vitae, certaines indications sur le patrimoine (numéros de compte, solde du compte, etc.) ainsi que les données sur les antécédents personnels et professionnels de la personne concernée (…) ».*

Ni les articles du projet de loi, ni le commentaire des articles ne font mention des catégories particulières de données à caractère personnel. Conformément à l'article 9 du RGPD, le traitement portant sur des catégories particulières de données à caractère personnel est interdit, sauf si l'une des conditions indiquées au paragraphe 2 dudit article est remplie, par exemple si le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État-membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée (article 9, paragraphe 2, lettre (g) du RGPD).

La CNPD rappelle encore que le traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions doit être autorisé par le droit de l'Union ou par le droit d'un État-membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées.

Elle ignore cependant si des dispositions législatives européennes ou nationales permettent à la CSSF ou au CAA de traiter des catégories particulières de données au sens de l'article 9 du RGPD, et si des garanties appropriées sont prévues dans ces dispositions législatives conformément aux exigences du paragraphe 2 lettre (g) de cet article.

[106] Projet de loi n°7373, doc. parl. 7373/00, p. 17.

Par exemple, pour ce qui est du casier judiciaire, le règlement grand-ducal modifié du 23 juillet 2016 fixant la liste des administrations et personnes morales de droit public pouvant demander un bulletin n°2 ou n°3 du casier judiciaire avec l'accord écrit ou électronique de la personne concernée autorise la CSSF à recevoir sur demande et avec l'accord exprès de façon écrite ou électronique de la personne concernée un casier judiciaire *« pour apprécier le respect de la condition de l'honorabilité professionnelle, conformément aux lois spéciales qui attribuent cette compétence à la Commission de Surveillance du Secteur financier ou à la Banque centrale européenne »* (article 1er, point 5). Le CAA, quant à lui, peut le recevoir *« pour l'instruction de toute demande d'agrément adressée à un service de sa compétence »* (article 1er, point 6).

III. <u>Le traitement à une fin autre que celle pour laquelle les données ont été collectées par la CSSF (article 16-2 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-2 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi)</u>

Le nouvel article 16-2 de la loi modifiée du 23 décembre 1998 et le nouvel article 13-2 de la loi modifiée du 7 décembre 2015, tels qu'insérés par le projet de loi, visent à permettre à la CSSF et le CAA de traiter des données à caractère personnel à des fins autres que celles pour lesquelles les données ont été collectées dans des cas spécifiques.

Conformément à l'article 5, paragraphe 1er, lettre (b) du RGPD, les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (principe de limitation des finalités). Selon son article 6, paragraphe 4, les données à caractère personnel peuvent néanmoins être traitées pour une finalité autre (même incompatible) que celle pour laquelle elles ont été collectées initialement, sur base du consentement de la personne concernée ou sur base du droit de l'Union ou de l'État-membre, qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1 du RGPD

La CNPD regrette ainsi que les auteurs du projet de loi n'aient pas expliqué de manière plus précise et concrète la nécessité des dispositions relatives au traitement ultérieur, qui permettent à la CSSF et au CAA de traiter les données pour une finalité autre que celle pour laquelle les données ont été collectées initalement. En effet, comme l'a précisé l'autorité de supervision irlandaise (Data Protection Commission), dans sa guidance relative à l'article 23 du RGPD, *« [a] proposed measure should be supported by evidence describing the problem to be addressed by the measure, how it will be addressed by the measure, and why existing or less intrusive measures cannot sufficiently address it »*[107]. Toute exception doit être nécessaire et proportionnelle eu égard aux missions de la CSSF ou du CAA.

Ainsi, en l'absence d'une délimitation plus précise des catégories de données qui pourraient faire l'objet d'un traitement ultérieur, et d'explications plus précises quant à la nécessité et la proportionnalité de ce

[107] Data Protection Commission Ireland, Limiting Data Subject Rights and the Application of Article 23 of the General Data Protection Regulation, https://www.dataprotection.ie/en/individuals/know-your-rights/restriction-individual-rights-certain-circumstances-article-23-gdpr

traitement dans le commentaire des articles, la CNPD n'est pas en mesure d'apprécier la conformité de la mise en œuvre pratique de ces dispositions au RGPD, alors que la disposition sous examen est trop générale et vague.

Indépendamment de la compatibilité du nouveau traitement avec le traitement initial, ce nouveau traitement doit satisfaire aux exigences du RGPD. Comme le précise le considérant 50 du RGPD, *« [e]n tout état de cause, l'application des principes énoncés dans le présent règlement et, en particulier, l'information de la personne concernée au sujet de ces autres finalités et de ses droits, y compris le droit de s'opposer au traitement, devraient être assurées»*.

Ainsi, tout traitement de données à une fin autre que celle pour laquelle les données ont été collectées doit respecter les principes du RGPD, comme par exemple, le principe de minimisation de données et l'obligation de faire figurer le traitement dans le registre des activités de traitement de la CSSF ou du CAA.

A l'instar de son homologue allemand, la CNPD suggère d'intégrer dans les dispositions sous revue une garantie supplémentaire prévoyant que le traitement ultérieur peut uniquement avoir lieu si l'intérêt public poursuivi par l'autorité, à savoir la CSSF ou le CAA, prime sur les droits et intérêts des personnes concernées[108].

Quant aux cas dans lesquels les données peuvent être traitées à des fins autres que celles pour lesquelles elles ont été collectées, la lettre (b) permettrait le traitement ultérieur pour assurer l'exercice des missions de la CSSF ou du CAA ainsi que le respect des obligations qui en découlent dans le chef de la CSSF ou du CAA, *« y compris en matière de coopération avec d'autres institutions, autorités, organes ou organismes nationaux, étrangers, européens ou internationaux, telle que prévue dans les lois sectorielles régissant lesdites missions »*. La Commission nationale estime que l'inclusion des mots « y compris » ne permet pas de délimiter avec suffisance les situations dans lesquelles les données pourraient faire l'objet d'un traitement ultérieur. En effet, cette formulation englobe toutes les missions et obligations de la CSSF et le CAA, y compris les cas de figure énumérés dans les articles sous revue. Il convient dès lors soit d'énumérer avec plus de précisions les missions et obligations de la CSSF et du CAA dans le cadre desquelles les données pourraient être traitées à des fins ultérieures, soit de supprimer ces mots de la disposition.

En ce qui concerne les lettres (b) et (c), la CNPD note que les lois sectorielles spécifiques contiennent généralement des dispositions relatives à la coopération entre la CSSF ou le CAA et d'autres institutions, autorités, organes et organismes nationaux et étrangers. Ces lois et leurs mesures d'exécution devraient faire référence aux dispositions légales régissant cette coopération ainsi que la base légale du transfert.

La CNPD rappelle encore que les transferts de données vers les pays tiers doivent être réalisés en conformité avec le chapitre V du RGPD.

[108] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Positionspapier zum Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, 3 mars 2017, p. 10-12.

Quant à la lettre (d), le commentaire des articles ne précise pas la nécessité de traiter des données à caractère personnel pour développer, contrôler et modifier des procédures internes de fonctionnement de la CSSF et du CAA. Pour le cas où il s'agirait des procédures automatisées, telles que visées par le texte allemand duquel les auteurs du projet de loi se sont inspirés[109], la CNPD recommande de prévoir, à l'instar dudit texte allemand, que les données soient uniquement utilisées à des fins de développement, de contrôle et de modification des procédures internes et soient effacées endéans un an après la fin des mesures de développement, de contrôle ou de modification.

Quant aux lettres (d) et (e), la CNPD s'interroge sur le sens de la formulation *« données personnelles non pseudonymisées »*. En effet, il est évident que des données « non pseudonymisées » sont des données « à caractère personnel ». Pourquoi alors ne pas employer la formulation du RGPD de « données à caractère personnel » ? Par ailleurs, il convient de rappeler que les données pseudonymisées sont également des données à caractère personnel, si elles peuvent *« être attribuées à une personne physique par le recours à des informations supplémentaires »* (considérant 26 du RGPD).

La CNPD s'interroge aussi sur la pertinence de la référence au RGPD au début des articles 16-2 de la loi modifiée du 23 décembre 1998 et 13-2 de la loi modifiée du 7 décembre 2015 (commençant tous deux par ces termes : « sans préjudice de l'article 6, paragraphe (4) du Règlement (UE) 2016/679 (…) »). En effet, ledit article du RGPD s'applique en tout état de cause à tout traitement à une fin autre que celle pour laquelle les données ont été collectées. La Commission nationale comprend donc que les articles 16-2 de la loi modifiée du 23 décembre 1998 et 13-2 de la loi modifiée du 7 décembre 2015 s'entendent en conformité ou en application (et non « sans préjudice ») de l'article 6, paragraphe (4) du RGPD.

Finalement, afin d'assurer une meilleure cohérence entre le vocabulaire utilisé dans le présent projet de loi et celui du RGPD, la CNPD propose d'amender l'intitulé de l'article 13-2 de la modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi et de le renommer « Traitement à une fin autre que celle pour laquelle les données ont été collectées ».

IV. La limitation du droit à l'information par la CSSF (articles 16-3 et 16-4 de la loi modifiée du 23 décembre 1998, tels qu'insérés par le projet de loi) et par le CAA (articles 13-3 et 13-4 de la loi modifiée du 7 décembre 2015, tels qu'insérés par le projet de loi)

Les articles sous revue visent à limiter l'obligation de la CSSF et du CAA de fournir aux personnes concernées certaines informations relatives aux traitements de données. Figurant à l'article 5, paragraphe 1er, lettre (a) du RGPD, le principe de transparence constitue un aspect fondamental des principes relatifs au traitement[110]. Cette information constitue souvent le premier contact entre le responsable du traitement et la personne concernée, que ce soit dans le cadre d'une collecte directe ou bien dans le cadre d'une collecte indirecte. Ainsi, *« [s]on objectif*

[109] Projet de loi n°7373, doc. parl. 7373/00, p. 16
[110] Groupe de travail « Article 29 » sur la protection des données, lignes directrices sur la transparence au sens du règlement (UE) 2016/679, adoptées le 11 avril 2018, disponible à l'adresse https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227, p. 5.

premier est de susciter la confiance dans les processus applicables aux citoyens en leur permettant de comprendre et, au besoin, de contester lesdits processus »[111].

Comme les limitations des droits des personnes concernées ne doivent pas dépasser ce qui est strictement nécessaire, la CNPD se félicite de la précision faite aux articles 16-3 et 16-4 de la loi modifiée du 23 décembre 1998 et aux articles 13-3 et 13-4 de la loi modifiée du 7 décembre 2015, selon laquelle la CSSF et le CAA ne peuvent pas avoir recours aux exceptions, sauf s'ils peuvent démontrer que l'intérêt public poursuivi par ces autorités prime sur les intérêts des personnes concernées. Afin de rappeler que les exceptions ne peuvent être prévues par le droit national que si elles sont nécessaires et proportionnelles dans une société démocratique, la CNPD recommande d'insérer une formulation identique dans les dispositions relatives à l'obligation d'information en cas de collecte directe. Il convient de rappeler que cette évaluation doit être consigné par écrit conformément à l'article 16-8, paragraphe (3) de la loi modifiée du 23 décembre 1998 et à l'article 13-8 paragraphe (3) de loi modifiée du 7 décembre 2015

La Commission nationale s'interroge cependant sur les formulations employées à la lettre (a), à savoir l'exercice des missions et compétences, et à la lettre (b), à savoir la stabilité du système bancaire et financier ou des marchés, le maintien de l'ordre public ou la sécurité publique. L'alinéa 1er de la lettre (a) et le commentaire des articles comportent une explication des situations visées par les dispositions. Ainsi dans le cadre de la lettre (a), cette exception vise principalement les contrôles, les enquêtes et les procédures de sanction de la CSSF et du CAA, ainsi que les actes préparatoires à de telles enquêtes[112]. Afin de limiter les limitations des droits au strict nécessaire, il importe de circonscrire de manière plus précise les cas dans lesquels les droits des personnes concernées peuvent être limités.

La CNPD s'interroge encore sur la nécessité de limiter le droit à l'information des personnes concernées, si le plein ou immédiat exercice des droits de la personne concernée ou des obligations de la CSSF ou du CAA *« porte atteinte à des intérêts légitimes protégés de tiers »*[113], si les données sont collectées directement auprès de la personne concernée. En effet, si la personne concernée transmet de manière directe les données à la CSSF et le CAA, la CNPD s'étonne du fait que la communication des informations relatives au traitement pourrait porter préjudice aux intérêts légitimes des tiers. Comme le commentaire des articles ne précise ni les intérêts légitimes, ni les tiers concernés, la CNPD se demande si cette disposition est limitée à ce qui est strictement nécessaire. Sans davantage de précisions et compte tenu de l'importance que le RGPD confère au droit à l'information pour les personnes concernées, la CNPD estime nécessaire de supprimer ces dispositions du projet de loi.

La limitation du droit à l'information des personnes concernées figure également à l'article 16-4 de la loi modifiée du 23 décembre 1998 et à l'article 13-4 de la loi modifiée du 7 décembre 2015, tels qu'insérés par le projet de loi, qui visent le cas de données à caractère personnel qui n'ont pas été collectées auprès de la personne concernée. Comme les auteurs visent notamment des données issues des lignes d'alertes (« whistleblowing hotlines »), la

[111] *Idem.*
[112] Projet de loi n°7373, doc. parl. 7373/00, p. 11-12.
[113] Lettre (f) de l'article 16-3 de la loi modifiée du 23 décembre 1998 et lettre (f) de l'article 13-3 de la loi modifiée du 7 décembre 2015, telles qu'insérées par le projet de loi.

Commission se permet de rappeler l'avis n°1/2006 du Groupe de travail « Article 29 », qui précise que la disposition relative aux informations à fournir aux personnes concernées, lorsque leurs données personnelles sont collectées auprès d'un tiers et non directement auprès d'elles, s'applique lorsqu'un informateur effectue un signalement concernant une tierce personne et fournit des données à caractère personnel relatives à cette dernière. La personne faisant l'objet d'un signalement devrait dès lors être informée dans les plus brefs délais après l'enregistrement des données la concernant. Alors que la notification peut être retardée s'il existe un risque sérieux qui compromettrait la capacité de l'organisme, dans le cas d'espèce la CSSF et le CAA, d'enquêter efficacement sur les faits allégués, ce cas de figure pourrait être couvert par l'exception prévue à la lettre (a).

V. La limitation du droit d'accès par la CSSF (article 16-5 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-5 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi)

L'article 16-5 de la loi modifiée du 23 décembre 1998 et l'article 13-5 de la loi modifiée du 7 décembre 2015 entendent permettre à la CSSF et au CAA de limiter le droit d'accès des personnes concernées.

La CNPD relève que les auteurs du projet ont entendu préciser que la limitation prévue par ces articles ne concerne que les paragraphes 1er et 2 de l'article 15 du RGPD. Une telle précision laisse entendre que le droit d'obtenir une copie des données faisant l'objet d'un traitement (article 15, paragraphe 3 du RGPD) ne ferait, quant à lui, pas l'objet de cette limitation.

La Commission nationale s'interroge sur la raison d'être de permettre à la CSSF et au CAA de limiter ou différer la confirmation à la personne concernée que des données à caractère personnel sont traitées et l'accès auxdites données, ainsi que de limiter ou différer la transmission de tout ou partie des informations visées à l'article 15, paragraphes 1er et 2 du RGPD, mais pas de limiter ou de différer le droit pour la personne concernée d'obtenir une copie des données faisant l'objet d'un traitement.

S'il s'agit d'un choix délibéré des auteurs du projet de loi, la Commission nationale aurait du mal à percevoir la réelle plus-value des exceptions visées à l'article 16-5 de la loi modifiée du 23 décembre 1998 et à l'article 13-5 de la loi modifiée du 7 décembre 2015, alors que la personne concernée disposera en tout état de cause du droit d'obtenir une copie des données traitées par la CSSF ou le CAA la concernant (sauf, bien évidemment, si ce droit d'obtenir une copie porterait atteinte aux droits et libertés d'autrui, conformément à l'article 15 paragraphe (4) du RGPD).

Faut-il au contraire comprendre que les lettres (c) des dispositions précitées s'étendent également au droit pour la personne concernée d'obtenir une copie des données faisant l'objet d'un traitement ? Si tel était le cas, la Commission nationale estimerait nécessaire, dans un souci de sécurité juridique, d'ajouter explicitement une

référence au paragraphe (3) de l'article 15 du RGPD dans ces dispositions, afin d'indiquer que cet aspect du droit d'accès est également couvert par les exceptions.

VI. <u>La limitation du droit à la limitation du traitement par la CSSF (article 16-6 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-6 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi)</u>

Les articles sous revue renvoient à l'article 16-6 de la loi modifiée du 23 décembre 1998 et à l'article 13-6 de la loi modifiée du 7 décembre 2015 pour énoncer les cas de figure qui permettraient à la CSSF et au CAA de limiter le droit à la limitation du traitement, en rajoutant également que les exceptions ne s'appliquent que pour autant que l'intérêt public poursuivi par la CSSF ou par le CAA *« de ne pas fournir à la personne concernée ces informations prime sur l'intérêt privé de la personne concernée »*. Le commentaire des articles ne fournit aucune précision relative à la nécessité de ces exceptions au droit à la limitation.

Il convient de noter qu'en tout état de cause, le droit à la limitation du traitement ne peut être exercé par la personne concernée que si sa demande est fondée sur l'une des hypothèses limitativement énumérées à l'article 18, paragraphe 1er du RGPD. Par ailleurs, même en cas d'exercice du droit à la limitation du traitement, les données peuvent être traitées sans limitation par le responsable du traitement dans les conditions énoncées au paragraphe 2 dudit article, par exemple, si le traitement est nécessaire pour des motifs importants d'intérêt public de l'Union ou d'un État-membre.

En l'absence de justification supplémentaire, la CNPD se demande dès lors quelle est la réelle plus-value de l'article 16-6 de la loi modifiée du 23 décembre 1998 et de l'article 13-6 de la loi modifiée du 7 décembre 2015, alors que l'application de l'article 18 du RGPD pourrait déjà faire obstacle, dans la plupart des cas, à l'exercice du droit à la limitation du traitement effectué par la CSSF ou la CAA.

VII. <u>La limitation du droit de s'opposer au traitement par la CSSF (article 16-7 de la loi modifiée du 23 décembre 1998, tel qu'inséré par le projet de loi) et par le CAA (article 13-7 de la loi modifiée du 7 décembre 2015, tel qu'inséré par le projet de loi)</u>

Les articles 16-7 de la loi modifiée du 23 décembre 1998 et 13-7 de la loi modifiée du 7 décembre 2015 permettraient à la CSSF et au CAA de limiter le droit de s'opposer aux traitements opérés par ces autorités les concernant, en précisant que ces limitations ne s'appliquent que pour autant que l'intérêt public poursuivi par la CSSF ou par le CAA *« de procéder au traitement prime sur l'intérêt privé de la personne concernée »*.

Dans le commentaire des articles, les auteurs du projet de loi précisent que ces articles *« concrétise[nt] l'exception prévue à la seconde phrase de l'article 21 du Règlement (UE) 2016/679 qui permet de ne pas donner suite à*

cette demande lorsqu'il existe des motifs légitimes et impérieux pour le traitement qui doivent prévaloir sur les intérêts et les droits et libertés de la personne concernée, pour la constatation, l'exercice ou la défense de droits en justice ». La Commission nationale relève que le droit de s'opposer à un traitement ne peut être exercé par la personne concernée sur base de l'article 21 du RGPD que *« pour des raisons tenant à sa situation particulière »*. Comme pour les autres limitations, il s'agit ainsi d'une analyse au cas par cas. La CNPD ne perçoit ainsi pas la réelle plus-value des articles sous revue par rapport à la seconde phrase de l'article 21, paragraphe (1) du RGPD.

VIII. <u>Les garanties (articles 16-8 et 16-9 de la loi modifiée du 23 décembre 1998, tels qu'insérés par le projet de loi, et articles 13-8 et 13-9 de loi modifiée du 7 décembre 2015, tels qu'insérés par le projet de loi)</u>

De manière générale, la Commission nationale se félicite des garanties substantielles apportées par les articles 16-8 et 16-9 de la loi modifiée du 23 décembre 1998 et par les articles 13-8 et 13-9 de loi modifiée du 7 décembre 2015.

En effet, comme plus amplement détaillé dans son avis du 29 mars 2018 (délibération n°219/2018), en cas de mise en œuvre des dérogations de l'article 23 du RGPD dans une loi nationale, il est indispensable de prévoir en contrepartie des garanties appropriées afin de ne pas remettre en cause l'essence des droits fondamentaux des personnes concernées.

En l'espèce, l'article 16-8 de la loi modifiée du 23 décembre 1998 et l'article 13-8 de loi modifiée du 7 décembre 2015 prévoient notamment que la limitation des droits serait limitée dans le temps, et que la CSSF ou le CAA puisse justifier et informer la personne concernée de l'existence de cette limitation ainsi que de la possibilité d'introduire une réclamation auprès de la CNPD et de former un recours juridictionnel.

Les mêmes articles, ainsi que l'article 16-9 de la loi modifiée du 23 décembre 1998 et l'article 13-9 de loi modifiée du 7 décembre 2015, prévoient cependant certaines exceptions à ces garanties *« lorsque ces informations (…) risquent de nuire à la finalité du traitement, de la limitation ou du retard, notamment lorsque ces informations violent le secret professionnel auquel [sont] tenu[s] [la CSSF et le CAA] en application de l'article 7, ou lorsque ces informations empêchent [la CSSF ou le CAA] de poursuivre une procédure administrative ou juridictionnelle à laquelle [la CSSF ou le CAA] [sont] partie »*. Par ailleurs, la Commission nationale prend acte de la formulation vague du projet de loi, selon laquelle l'exercice des droits limités ou différés de la personne concernée pourrait trouver obstacle lorsque cela contreviendrait au secret professionnel auquel sont soumis tant les agents de la CSSF que ceux du CAA. Alors que la CNPD comprend la raison d'être de ces exceptions aux garanties, elle s'interroge sur l'inclusion du terme « notamment », qui laisse supposer que d'autres cas de figure pourraient permettre à la CSSF et au CAA de faire obstacle aux droits et aux garanties prévues par les articles en question. Etant donné que ces garanties visent à assurer un socle de protection élémentaire pour les personnes concernées dans les cas où leurs droits consacrés par le RGPD seraient limités, il convient de restreindre les

exceptions au strict nécessaire. Dès lors, si les auteurs du projet de loi entendent viser d'autres exceptions, la CNPD estime nécessaire de les inclure dans le texte de ces articles.

En outre, la Commission nationale note que la CSSF et le CAA doivent consigner *« par écrit les motifs de fait et de droit sur lesquels se fonde sa décision de limiter ou de différer les droits de la personne concernée ou ses propres obligations… »* (article 16-8, paragraphe (3) de la loi modifiée du 23 décembre 1998 et article 13-8 paragraphe (3) de loi modifiée du 7 décembre 2015). Ces informations doivent être tenues à la disposition de la CNPD, *« sans préjudice de l'obligation du secret professionnel »* de la CSSF et du CAA. La CNPD ne voit cependant pas en quoi l'obligation du secret professionnel de ces autorités pourrait faire obstacle à ses missions légales de contrôles, qui consistent notamment à vérifier la licéité des traitements effectués par les responsables de traitements du secteur privé et public. Sans explication supplémentaire des auteurs du projet de loi, la CNPD estime donc que ces termes devraient être supprimés du texte du projet de loi. Par ailleurs, il convient de rappeler que les agents de la Commission nationale sont eux-mêmes soumis au secret professionnel, conformément à 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 selon lequel *« sans préjudice de l'article 23 du Code de procédure pénale, toutes les personnes exerçant ou ayant exercé une activité pour la CNPD sont tenues au secret professionnel et passibles des peines prévues à l'article 458 du Code pénal en cas de violation de ce secret »*.

En outre, les seules restrictions aux pouvoirs de contrôle de la CNPD lui conférés par l'article 58 du RGPD et relatives au secret professionnel sont celles limitativement énumérés à l'article 67 de la loi précitée du 1er août 2018. De l'avis de la Commission nationale, le secret professionnel auquel sont soumis la CSSF et le CAA ne peut donc pas faire obstacle aux missions légales de contrôles de la CNPD.

La CNPD s'interroge sur l'utilisation des termes « ces informations », alors que l'alinéa précédent concerne tant les motifs de fait et de droit sur lesquels est fondée la décision de la CSSF ou du CAA de restreindre les droits des personnes concernées, que la précision de la date de fin de la limitation. Dans un souci de sécurité juridique, il convient de préciser que la CNPD peut recevoir communication de toutes les informations concernant la limitation d'un droit d'une personne concernée.

Par ailleurs, l'article 16-9 de la loi modifiée du 23 décembre 1998 et l'article 13 paragraphe (9) de loi modifiée du 7 décembre 2015 entendent permettre que les droits limités ou différés de la personne concernée soient exercés par la CNPD, qui interviendrait en quelque sorte comme intermédiaire entre la personne concernée d'une part, et la CSSF ou le CAA d'autre part. Aux yeux de la CNPD, ce mécanisme constitue une garantie appropriée afin de compenser l'absence ou la limitation des droits « directs » des citoyens envers la CSSF ou du CAA. Il est à noter qu'un « droit d'accès indirect » existait d'ailleurs déjà dans le cadre de la loi modifiée de 2002, pour garantir aux personnes concernées qu'une autorité de contrôle indépendante, en l'occurrence la CNPD, puisse vérifier la licéité du traitement[114].

[114] Cf. article 29 paragraphe (5) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

IX. Article III

Les commentaires énoncés aux sections I à VIII du présent avis sont également applicables aux articles 105 et 154 de la loi modifiée du 18 décembre 2018 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement. La Commission nationale note notamment que le commentaire des articles ne précise pas la nécessité des limitations pour le Fonds de Garantie des Dépôts Luxembourg et pour le Fonds de Résolution Luxembourg.

X. Considérations finales

Alors que la CNPD peut comprendre la raison d'être des limitations aux droits des personnes concernées évoquées ci-dessus afin de ne pas compromettre une enquête ou un contrôle de la CSSF ou du CAA, elle se demande s'il n'y aurait pas lieu de préciser qu'elles ne visent pas les données qui sont étrangères à l'objet de l'enquête ou du contrôle justifiant ces limitations. A cet égard, elle se réfère à l'avis de ses homologues belges du 11 avril 2018[115], lesquels proposent une délimitation claire du champ d'application matériel de toute exception qui exécute l'article 23 du RGPD dans la législation sectorielle applicable, en proposant par exemple une formulation du type : *« ces dérogations valent dans la mesure où l'application de ce droit nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires ou risque de violer le secret de l'enquête pénale. La restriction visée au paragraphe 1er, alinéa 1er, ne vise pas les données qui sont étrangères à l'objet de l'enquête ou du contrôle justifiant le refus ou la limitation d'accès ».*

Par ailleurs, ni le projet de loi ni le commentaire des articles n'aborde les risques potentiels pour les droits et libertés des personnes concernées dont les données pourraient être traitées par la CSSF ou par le CAA. Afin d'assurer la conformité à l'article 23 paragraphe (2) lettre (g), il convient d'identifier plus clairement les risques que les auteurs du projet de loi souhaitent palier dans le cadre du projet de loi.

Ainsi décidé à Esch-sur-Alzette en date du 5 avril 2019.

La Commission nationale pour la protection des données,

Tine A. Larsen	Thierry Lallemang	Christophe Buschmann
Présidente	Commissaire	Commissaire

[115] Autorité de protection des données (anciennement Commission de la protection de la vie privée), avis 33/2018 du 11 avril 2018, disponible à l'adresse https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_33_2018.pdf, p. 42.

Avis de la Commission nationale pour la protection des données relatif au recours à la vidéosurveillance par les communes.

Délibération n°39/2019 du 10 mai 2019

Conformément à l'article 57, paragraphe 1er lettre c) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données (ci- après désigné « 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 ».

Eu égard à la mission de conseil qui lui est attribuée, mais également suite à la requête de Madame la Ministre de l'Intérieur concernant les conditions d'installations de caméras de vidéosurveillance au sein des communes et face aux interrogations des bourgmestres à ce sujet, la Commission nationale rend un avis circonstancié quant au recours à la vidéosurveillance par les communes.

A titre liminaire, la CNPD constate que les communes, dans leurs demandes d'informations quant à l'installation de dispositifs de vidéosurveillance dans l'espace public, font référence à l'ancien régime de protection des données. Un bref retour en arrière est donc nécessaire afin de comprendre les tenants et les aboutissants du cadre légal actuellement en vigueur.

La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, en particulier les articles 10 et 11, prévoyait des dispositions spécifiques relatives à la surveillance. L'article 14 de cette loi prévoyait quant à lui, l'obligation de demander une autorisation auprès de la CNPD avant toutes installations de dispositifs de vidéosurveillance. L'article 17 de cette même loi était le fondement légal de la surveillance de l'espace public effectuée par la Police grand-ducale.

Aujourd'hui, la saisie de la CNPD par Madame la Ministre de l'Intérieur intervient au lendemain de l'entrée en application du nouveau « paquet protection des données » composé d'un règlement général pour la protection des données[116] (ci-après désigné « RGPD ») et d'une directive relative à la protection des données dans les domaines relatifs à la police et la justice[117] (ci-après désignée « la directive police-justice »). Ces deux textes ont des champs d'application distincts mais néanmoins complémentaires.

[116] 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, JO L119, 4.5.2016, p.1-88.

[117] 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, JO L119, 4.5.2016, p. 89-131.

ANNEXES

5

Le RGPD est directement applicable dans la législation luxembourgeoise. La loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données a abrogé la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. La nouvelle législation a supprimé l'obligation pour les responsables de traitement de données à caractère personnel d'effectuer une demande d'autorisation à la CNPD avant l'installation de dispositifs de vidéosurveillance. Les communes, en tant que responsables de traitement[118] sont à présent tenues de respecter les principes[119] et obligations consacrés par le RGPD lorsqu'elles mettent en place des systèmes de vidéosurveillance.

A ce titre et suite à l'entrée en vigueur de la nouvelle législation, la CNPD a publié au mois d'août 2018 des lignes directrices en matière de vidéosurveillance (ci-après désignées « les lignes directrices »). Sans vouloir prétendre à l'exhaustivité, la CNPD y a rappelé certains principes et certaines obligations applicables en matière de vidéosurveillance. Par conséquent, les communes peuvent se référer aux lignes directrices dont une copie est fournie en annexe[120] du présent avis, afin d'avoir un aperçu des règles applicables en la matière.

Afin de bien saisir les enjeux que soulèvent l'installation et l'exploitation des dispositifs de vidéosurveillance au sein des communes et les problématiques qui en émanent, il y a lieu d'effectuer une distinction entre les lieux surveillés d'une part, et les finalités poursuivies par le responsable de traitement lors du recours auxdits dispositifs d'autre part. Ces enjeux et problématiques peuvent être mis en lumière à travers trois exemples développés ci-dessous.

Lorsqu'une commune souhaite surveiller un bâtiment ou d'autres installations communales à des fins de protection des biens et/ou de sécurité des usagers, une telle surveillance intervient dans le cadre des missions « classiques » reconnues à celle-ci. Avant l'entrée en application du RGPD et sous l'égide de la loi de 2002, la CNPD autorisait la surveillance de ces zones sous réserve du respect de certaines conditions et obligations. Aujourd'hui, la commune est tenue de respecter les principes et les obligations du RGPD, qui d'ailleurs, n'ont pas changé par rapport à l'ancienne législation. A titre d'exemples, la CNPD considère que l'installation d'un dispositif de vidéosurveillance est en principe proportionnée aux entrées et aux sorties de bâtiments, aux alentours immédiats de ces derniers, dans des locaux de stockage, aux zones de livraisons et de chargements[121] etc. Le caractère proportionné réside dans le fait que les zones surveillées sont restreintes et les personnes qui y sont présentes telles que les visiteurs, les clients ou encore les employés, ne sont pas soumis à une surveillance permanente.

Lorsqu'une commune souhaite installer des dispositifs de vidéosurveillance au sein de l'espace public, la zone surveillée est en principe plus étendue. Le champ de vision du dispositif couvre des surfaces beaucoup plus grandes telles que des places publiques, des parcs, des aires de jeux ouvertes à tous ou encore des rues. Avant l'entrée en application du RGPD et conformément à la loi de 2002, la CNPD n'autorisait pas la

[118] Une définition de ce qu'est un responsable de traitement est donnée à l'article 3. 7) 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, JO L119, 4.5.2016, p.1-88.
[119] *Ibidem,* article 5 et suivants.
[120] Annexe I.
[121] Lignes directrices en matière de vidéosurveillance, p.8.

surveillance de ces zones considérant que la protection des intérêts des citoyens prévalait sur la protection des biens et la sécurité des usagers. En ce qui concerne les aires de jeux, en particulier, la CNPD a toujours considéré que l'installation et l'exploitation de vidéosurveillance étaient attentatoire à la vie privée puisqu'il s'agissait là d'espaces de vie, de loisirs et de récréation dans lesquels l'on pouvait légitimement s'attendre à ne pas être filmé et surveillé en permanence pendant le temps de présence dans ces espaces. Sous l'égide du cadre légal actuel, la position de la CNPD reste en principe inchangée. Dans ses lignes directrices et conformément au RGPD, la CNPD considère qu'au sein de ces zones, l'installation de caméras est disproportionnée par rapport aux buts poursuivis. En effet, la surveillance qui en émane porte sur un nombre conséquent d'individus qui circulent au sein de l'espace public et cette surveillance n'est pas limitée dans le temps.

En outre, la CNPD constate qu'il ressort des demandes d'avis de la part des communes que celles-ci souhaitent installer des dispositifs de vidéosurveillance à des fins de prévention et de détection d'infractions pénales. Il apparaît en effet que ces dernières ont l'intention de lutter contre des actes de délinquance, de vandalisme etc., d'autant plus que certaines communes ont manifesté leur souhait d'être reliées au système VISUPOL, exploité par la Police grand-ducale actuellement limité au seul territoire de la Ville de Luxembourg. Or, dans une telle hypothèse, c'est un autre régime légal qui s'applique en matière de protection des données. Il s'agit en effet 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[122]. Cette loi transpose la directive police-justice[123] précitée en droit national.

A cet égard, la Commission nationale pour la protection des données a rendu le 15 mars 2019 un avis relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique[124] dont une copie est également fournie en annexe[125]. Celui-ci peut être très utile aux communes souhaitant installer un dispositif de vidéosurveillance à des fins de sécurité publique et doit être lu de concert avec les présents développements.

La CNPD souhaite attirer l'attention sur le fait que la finalité du traitement poursuivie par le responsable du traitement, en l'espèce la commune, doit entrer dans le champ de compétence de celui-ci. Comme l'indique le Groupe de travail « article 29 » : « il faudra tenir compte des fonctions publiques qui ne peuvent être exercées, aux termes de la loi, que par des organismes spécifiques non administratifs tels que, en particulier, des organismes de police et/ou l'autorité judiciaire »[126]. Autrement dit, une commune ne peut outrepasser ses compétences et installer un système de vidéosurveillance pour une finalité qui relève des compétences de la Police grand-ducale.

La CNPD constate cependant que si la loi communale et la loi sur la Police grand-ducale mettent en exergue les interactions entre la police et les bourgmestres, aucune des deux ne précisent les compétences des bourgmestres en matière de police. En effet, la loi communale renseigne sur les attributions des bourgmestres[127] et sur l'interaction

[122] 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 portant modification de certaines lois.
[123] 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, JO L119, 4.5.2016, p. 89-131.
[124] Avis de la Commission nationale pour la protection des données relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique, Délibération n°36/2019 du 15 mars 2019.
[125] Annexe II.
[126] Avis 4/2004 du groupe de travail « Article 29 » sur le traitement des données à caractère personnel au moyen de la vidéosurveillance, p.14, disponible à l'adresse suivante : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp089_fr.pdf
[127] Loi communale du 13 décembre 1988, article 67.
[128] *Ibidem,* article 68.

entre ces derniers et la Police grand-ducale[128]. La loi du 18 juillet 2018 sur la Police grand-ducale[129] (ci-après désignée « loi sur la Police grand-ducale ») quant à elle, fait également part des interactions entre la police et les autorités communales. Il y est fait état des relations étroites entre les bourgmestres et les directeurs des régions de Police et les chefs des commissariats de police[130]. Or, ces dispositions légales ne permettent pas de délimiter clairement les compétences des bourgmestres de celles de la Police grand-ducale.

La CNPD souhaite également relever qu'un tel manque de précision se conjugue avec l'absence de base légale spécifique en matière de vidéosurveillance ne permettant pas de remplir les impératifs de prévisibilité et de qualité de la loi tels qu'ils sont consacrés par le droit de l'Union européenne et la jurisprudence des hautes juridictions européennes[131].

Conclusion

Dans son avis précité du 15 mars 2019, la CNPD est venue à la conclusion que, quel que soit le responsable du traitement, qu'il s'agisse d'une commune ou de la Police grand-ducale, les conditions et les modalités de mise en place de dispositifs de vidéosurveillance dans les espaces et lieux publics à des fins de sécurité publique devraient être précisés dans un cadre légal spécifique à l'instar d'autres pays européens comme par exemple la France, la Belgique et l'Allemagne. Dans ce contexte, elle a également salué la récente déclaration du Ministre de la sécurité intérieure qui considère *« qu'il est opportun de réfléchir à la mise en place d'un cadre légal spécifique pour l'installation future de caméras de surveillance »*[132].

Dans le cadre du présent avis, la CNPD ne peut que réitérer sa recommandation au gouvernement d'introduire en ce sens un cadre législatif spécifique, lequel pourrait intégrer et clarifier les interactions et les compétences respectives des bourgmestres et de la Police grand-ducale.

Ainsi décidé à Esch-sur-Alzette en date du 10 mai 2019.

La Commission nationale pour la protection des données,

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

[129] Loi du 18 juillet 2018 sur la Police grand-ducale et portant modification : 1° du Code de procédure pénale ; 2° de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État ; 3° de la loi du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 4° de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 5° de la loi du 18 décembre 2015 relative à l'accueil des demandeurs de protection internationale et de protection temporaire, et modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat ; et portant abrogation : 1° de la loi du 29 mai 1992 relative au Service de Police Judiciaire et modifiant 1. La loi du 23 juillet 1952 concernant l'organisation militaire ; 2. Le code d'instruction criminelle ; 3. La loi du 16 avril 1979 ayant pour objet la discipline dans la Force publique ; 2° de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

[130] *Ibidem,* articles 35 et 36.

[131] Les développements concernant les critères de prévisibilité et de qualité de la loi peuvent être retrouvés au sein de l'avis de la Commission nationale pour la protection des données relatif à la vidéosurveillance des espaces et lieux publics à des fins de sécurité publique, Délibération n°36/2019 du 15 mars 2019, pages 7 et suivantes.

[132] Communiqué par le ministère de la Sécurité intérieure du 12/03/2019, disponible à la page : https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2019/03-mars/12-bausch-videoprotection.html, consultée pour la dernière fois le 12/03/2019.

Avis 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°40/2019 du 5 juin 2019

Conformément à l'article 57, paragraphe 1, lettre 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 (ci-après : « le RGPD »), chaque autorité de contrôle a, dans le cadre du champ d'application du RGPD, pour mission de conseiller « conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ». L'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après : « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

Conformément à l'article 8, point 3°, de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la CNPD a, dans le cadre 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, notamment pour mission de *« conseille[r] 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 »*[133].

Par courrier du 15 mars 2019, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n°7424 portant création d'une plateforme commune de transmission électronique sécurisée et modification : 1. du code de procédure pénale, 2. de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État (ci-après : « le projet de loi »).

Il résulte de l'exposé des motifs que le projet de loi vise à mettre en place une plateforme commune et unique de transmission électronique sécurisée servant aux autorités judiciaires ainsi qu'au Service de renseignement de l'État (ci-après : « la plateforme »). Selon les auteurs du projet de loi, la plateforme offre une protection accrue des données personnelles des personnes faisant l'objet de mesures de repérage, de surveillance ou de contrôle.

[133] En ce qui concerne les champs d'application respectifs 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, voir notamment : D. Jeitz et T.A. Larsen, « Le futur régime de la protection des données dans les secteurs judiciaire et policier », Journal des tribunaux Luxembourg, n°54, 5 décembre 2017, pages 168-175.

La Commission nationale constate toutefois que le projet de loi reste muet sur les mesures techniques et organisationnelles à mettre en place pour garantir un niveau de sécurité adapté au regard de la sensibilité des données transmises via la plateforme, d'autant plus que le titre du projet de loi annonce la création d'une plateforme électronique « sécurisée ». De plus, elle regrette que le projet de règlement grand-ducal qui est censé définir le format et les modalités d'exécution suivant lesquelles les données collectées sont à transmettre respectivement aux autorités judiciaires et au Service de renseignement de l'État n'a pas été annexé au projet de loi.

La CNPD souhaite formuler des commentaires et réflexions sur le projet de loi, en suivant pour cela l'ordre de rédaction du texte.

I. Champ d'application

L'article 1 du projet de loi définit le champ d'application du texte sous examen en renvoyant à plusieurs articles du Code de procédure pénale ainsi qu'à l'article 7 de la loi modifiée du 5 juillet 2016 portant organisation du Service de renseignement de l'État (ci-après : « la loi du 5 juillet 2016 »).

Avant de se pencher sur le moyen technique permettant aux autorités judiciaires et au Service de renseignement de l'État d'accéder aux données conservées par les fournisseurs de réseau de communication public ou de services de communications électroniques, la Commission nationale souhaite formuler des observations sur le principe même de la conservation et de l'accès aux données de trafic et de localisation relatives aux communications électroniques.

A. L'article 43-1 du Code de procédure pénale

En cas de disparition d'une personne, l'article 43-1, alinéa 1, du Code de procédure pénale permet aux officiers de police judiciaire de procéder, sur instructions du procureur d'Etat, aux actes prévus aux articles 31 à 41 du Code de procédure pénale, c'est-à-dire aux actes prévus en cas de flagrant crime ou délit, aux fins de découvrir la personne disparue.

Or, contrairement à ce qui est indiqué à l'article 3, paragraphe 1, point 1°, du projet de loi, ni l'article 43-1 ni les articles 31 à 41 du Code de procédure pénale ne semblent prévoir de « procédure de localisation ».

A toutes fins utiles, la Commission nationale se permet de renvoyer à un arrêt de la Cour d'appel du 26 février 2008 selon lequel *« le repérage est depuis l'entrée en vigueur de l'article 67-1 réservé à la compétence exclusive du juge d'instruction »* de sorte que l'article 67-1 *« n'autorise pas les officiers de police judiciaire, agissant en vertu des pouvoirs qui leur sont spécialement conférés au titre des crimes et des délits flagrants, à opérer un tel repérage au titre des articles 33 et 31 du [Code d'instruction criminelle (actuellement Code de procédure pénale)] »*[134].

[134] Cour d'appel, cinquième chambre, 26 février 2008, arrêt 106/08 V.

Par ailleurs, la loi du 24 juillet 2010 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 (ci-après : « la loi du 24 juillet 2010 ») a modifié, suite à la recommandation formulée par la Commission nationale dans son avis du 26 avril 2010[135], le paragraphe 2 des articles 5 et 9 de la loi modifiée du 30 mai 2005 *« pour en assurer la cohérence avec l'article 67-1 du Code d'instruction criminelle aux termes duquel le repérage des communications n'est possible que s'il est ordonné par le juge d'instruction »*[136].

La CNPD se pose dès lors la question de savoir dans quelle mesure le projet de loi est susceptible de s'appliquer aux mesures ordonnées sur base de l'article 43-1 du Code de procédure pénale, respectivement quelle est précisément la *« procédure de localisation prévue par l'article 43-1 du Code de procédure pénale »*.

B. Les articles 67-1 et 88-1 du Code de procédure pénale

L'article 67-1 du Code de procédure pénale autorise le juge d'instruction de faire procéder au repérage des données d'appel de moyens de télécommunications à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés ainsi qu'à la localisation de l'origine ou de la destination de télécommunications.

L'article 88-1 du Code de procédure pénale, quant à lui, prévoit notamment la possibilité pour le juge d'instruction d'ordonner la surveillance et le contrôle des télécommunications ainsi que de la correspondance postale.

Dans le cadre des mesures prévues aux articles 67-1 et 88-1 du Code de procédure pénale, les autorités judiciaires peuvent être amenées à accéder aux données de trafic ou de localisation que les fournisseurs de service ou les opérateurs sont obligées de conserver en vertu 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 (ci-après : « la loi modifiée du 30 mai 2005 »).

L'obligation de conservation des données de trafic et de localisation relatives aux communications électroniques a été introduite dans notre législation nationale par la loi modifiée du 30 mai 2005, cela sur base de l'article 15, paragraphe 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 (ci-après : « la directive 2002/58/CE »).

L'article 15, paragraphe 1, de la directive 2002/58/CE permet une telle mesure lorsqu'une telle limitation des principes prévus aux articles 5,6,8 et 9 constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique notamment pour sauvegarder la sûreté de l'État ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.

[135] Délibération n°85/2010 du 26 avril 2010, point I. B. 2. : https://cnpd.public.lu/dam-assets/fr/decisions-avis/2010/retention-donnes/avis_CNPD_projet_loi_6113.pdf
[136] Projet de loi n°6113/8, p. 2.

ANNEXES

5

Par la suite, la loi du 24 juillet 2010 a transposé 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 2006/24/CE ») en modifiant la loi modifiée du 30 mai 2005.

Or, par arrêt du 8 avril 2014, la Cour de justice de l'Union européenne (ci-après : « la CJUE ») a déclaré invalide la directive 2006/24/CE en ce que le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7 (respect de la vie privée et familiale), 8 (protection des données à caractère personnel) et 52, paragraphe 1 (portée et interprétation des droits et des principes), de la Charte des droits fondamentaux de l'Union européenne[137].

La CJUE critique notamment que :

- la directive 2006/24/CE *« couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées de fonction de l'objectif de lutte contre les infractions graves »*[138] ;

- la directive 2006/24/CE *« ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence »*[139] ;

- en ce qui concerne les règles visant la sécurité et la protection des données conservées, la directive 2006/24/CE *« ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »*[140].

Suite à l'arrêt précité, le Ministre de la Justice a sollicité l'avis de la CNPD sur la conformité de la loi modifiée du 30 mai 2005 et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt de la CJUE du 8 avril 2014. Dans son avis du 13 mai 2014, la Commission nationale a recommandé de modifier les dispositions nationales afin de les rendre conformes aux exigences posées par ledit arrêt[141]. La CNPD a réitéré ces observations dans son avis relatif au projet de loi n°6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005[142].

Par la suite, l'arrêt de la CJUE du 21 décembre 2016[143] a encore une fois mis en avant la nécessité de modifier les dispositions nationales en statuant que :

[137] CJUE, 8 avril 2014, Digital Rights Ltd, affaires jointes C-293/12 et C-594/12.
[138] *Ibid.*, point 57.
[139] *Ibid.*, point 60.
[140] *Ibid.*, point 66.
[141] Délibération n°214/2014 du 13 mai 2014 : https://cnpd.public.lu/dam-assets/fr/decisions-avis/2014/Vorratsdatenspeicherung/214-2014-Deliberation-Ministere-Justice-avis-loi-modifiee-30-mai-2005-arret-CJUE-8-avril-2014-affaires-jointes-C-293-12-et-C-594-12-conservation-donnees.pdf
[142] Délibération n°228/2015 du 19 juin 2015 : https://cnpd.public.lu/dam-assets/fr/decisions-avis/2015/communications-electroniques/228_2015_Ministere-Justice_avis-projet-loi-modif-loi-communications-electroniques.pdf
[143] CJUE, 21 décembre 2016, Tele2 Sverige AB, affaires jointes C-203/15 et C-698/15.

- l'article 15, paragraphe 1, de la directive 2002/58/CE *« doit être interprété en ce sens qu'il s'oppose à une règlementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique » ;*

- l'article 15, paragraphe 1, de la directive 2002/58/CE *« doit être interprété en ce sens qu'il s'oppose à une règlementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union ».*

La CNPD estime dès lors qu'il y a lieu de de modifier et d'adapter le cadre législatif national afin d'assurer qu'il soit conforme à la jurisprudence de la CJUE.

Cette remarque vaut également pour l'article 7 de la loi du 5 juillet 2016 pour autant que le Service de renseignement de l'État puisse être amené à accéder aux données de trafic et de localisation conservées en vertu des articles 5 et 9 de la loi modifiée du 30 mai 2005.

En ce qui concerne le renvoi à l'article 88-1, paragraphe 1, du Code de procédure pénale, il serait opportun de clarifier si le projet de loi ne s'applique qu'à la surveillance et du contrôle des télécommunications ainsi que de la correspondance postale, ou également aux autres mesures prévues par cette disposition, à savoir la sonorisation et la fixation d'images de certains lieux ou véhicules ainsi que la captation de données informatiques.

II. Définitions

L'article 2, point 4°, du projet de loi fournit une définition de la notion d'« opérateur » en renvoyant à la définition prévue par la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques selon laquelle l' « opérateur » est une entreprise notifiée qui fournit ou est autorisée à fournir un réseau de communications public ou une ressource associée.

Ainsi, la notion d'« opérateur » est utilisée à l'article 3 du projet de loi tandis que les articles 4 et 5 emploient les notions d'« opérateurs de télécommunications » et de « fournisseurs d'un service de télécommunications », respectivement d'« opérateur des postes et télécommunications ».

La Commission nationale s'interroge pourquoi le projet de loi utilise des terminologies différentes.

Dans l'hypothèse où l'intention des auteurs du projet de loi serait d'utiliser les mêmes termes que ceux actuellement utilisés aux articles 67-1 du Code de procédure pénale et 7 de la loi du 5 juillet 2016, la Commission nationale se permet de renvoyer à son avis relatif au projet de loi n°6921 dans lequel elle a recommandé que la terminologie utilisée dans le Code d'instruction criminelle soit alignée sur celle d'ores et déjà utilisée dans la législation européenne et nationale[144].

En effet, la loi modifiée du 30 mai 2005, qui transpose plusieurs directives européennes, fait état d'opérateurs (de réseau) et de fournisseurs de services (de communications électroniques).

La CNPD suggère dès lors d'utiliser une terminologie uniformisée dans les différents textes.

III. Plateforme commune de transmission électronique sécurisée

A titre liminaire, la Commission nationale constate que la numérotation des paragraphes de l'article 3 du projet de loi semble erronée. Dans la suite de cet avis, elle utilisera une numérotation continue des paragraphes.

A. Quant à la qualification de responsable du traitement et de sous-traitant

L'article 3, paragraphe 2, du projet de loi dispose que la plateforme est hébergée auprès du Centre des technologies de l'information de l'État (ci-après : « le CTIE ») qui en assure la gestion opérationnelle.

Le paragraphe 3 du même article poursuit que le CTIE a la qualité de sous-traitant sans toutefois préciser quelle(s) autorité(s) est/sont à considérer comme responsable du traitement.

Dans le commentaire des articles, les auteurs du projet de loi indiquent que *« [l]es autorités judiciaires et le Service de renseignement de l'État sont responsables du traitement pour chaque donnée à caractère personnel qui les concerne »*. La Commission nationale estime que cette formulation peut prêter à confusion.

En effet, 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 (ci-après : « la loi du 1er août 2018 »), transposant 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, définit le responsable du traitement comme *« l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel »*.

[144] Délibération n°147/2016 du 12 février 2016, point 1 : https://cnpd.public.lu/dam-assets/fr/decisions-avis/2016/lutte-terrorisme/147-2016-PL6921.pdf

La personne concernée, par contre, désigne la personne physique identifiée ou identifiable à laquelle les données à caractère personnel se rapportent[145]. Il ne paraît dès lors pas approprié de prévoir que les autorités judiciaires et le Service de renseignement de l'État sont responsables du traitement pour les données qui les « concernent ». La CNPD comprend que chaque organisme est responsable pour la partie du traitement de données qui le concerne.

Le sous-traitant, quant à lui, est défini 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* »[146]. L'article 21 de la loi du 1er août 2018 traite plus particulièrement des relations entre le responsable du traitement et le sous-traitant.

La détermination du responsable du traitement revêt une importance particulière dans la mesure où il incombe notamment au responsable du traitement d'assurer le respect des principes énumérés à l'article 3 de la loi du 1er août 2018 et d'assurer les droits des personnes concernées conformément aux articles 11 et suivants de la loi du 1er août 2018.

La Commission nationale préconise partant que le projet de loi détermine clairement quelle(s) autorité(s) agi(ssen)t en tant que responsable du traitement. L'article 20 de la loi du 1er août 2018 prévoit d'ailleurs la possibilité que plusieurs autorités compétentes agissent comme responsables conjoints du traitement.

B. Quant aux éléments transmis aux opérateurs

Il ressort de l'article 3, paragraphe 4, du projet de loi et du commentaire y afférent que les opérateurs ne se voient plus communiquer les décisions ordonnant les mesures de repérage, de contrôle ou de surveillance, mais uniquement les éléments et informations techniques nécessaires à l'exécution des mesures.

La Commission nationale regrette que le projet de loi ne précise pas davantage quels éléments et informations techniques seront transmis par les autorités judiciaires et le Service de renseignement de l'État.

Par ailleurs, la Commission nationale se demande si le fait de ne plus communiquer l'ordonnance elle-même ne porte pas indûment atteinte au droit des opérateurs de former, le cas échéant, un recours contre les décisions ordonnant les mesures de repérage, de contrôle ou de surveillance.

C. Quant aux fichiers de journalisation des accès

Selon l'article 3, paragraphe 5, du projet de loi, « *[l]es informations relatives aux transmissions visées au paragraphe (4), à la personne ayant procédé à la consultation, aux informations consultées, aux critères de*

[145] Article 2, paragraphe 1, point 1°, de la loi du 1er août 2018.
[146] Article 2, paragraphe 1, point 9°, de la loi du 1er août 2018.

recherche, à la date et l'heure de la consultation ainsi qu'au motif de consultation sont conservées 12 mois à compter du jour où la mesure a été exécutée ».

Le commentaire des articles précise que ces fichiers de journalisation des accès (ci-après : « log files ») sont nécessaires à la vérification de la légalité des opérations effectuées.

La Commission nationale se félicite que le projet de loi prévoit le principe du contrôle de l'accès aux données par le biais de la journalisation. Elle s'interroge toutefois si la durée de conservation prévue au projet de loi est conforme aux exigences posées par la CJUE dans son arrêt du 7 mai 2009[147].

En effet, les personnes concernées ont, en vertu du droit d'accès, notamment le droit d'obtenir du responsable du traitement des informations relatives aux destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été communiquées.

Dans l'affaire ayant donné lieu à l'arrêt précité du 7 mai 2009, la personne concernée désirait connaître l'identité des personnes tierces auxquelles des informations la concernant avaient été communiquées au cours des deux années précédant sa demande ainsi que le contenu de l'information qui leur a été transmise. Il ressort de l'arrêt précité que les communications des données sont enregistrées selon un système automatisé mais que les données demandées par la personne concernée, antérieure à l'année précédant sa demande, ont été automatiquement effacées, ce qui serait conforme à la législation nationale applicable.

Selon la CJUE, *« [i]l appartient aux États-membres de fixer un délai de conservation de cette information [sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée] ainsi qu'un accès corrélatif à celle-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention et de recours prévus par la directive [95/46/CE] et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement »*[148].

La Cour a conclu que *« [u]ne 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 intérêt et obligation 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 »*[149].

Par ailleurs, l'effacement des log files après 12 mois est susceptible de rendre impossibles les poursuites judiciaires relatives à des violations du secret professionnel. En effet, tant les articles 67-1 et 88-4 du Code de procédure

[147] CJUE, 7 mai 2009, affaire C-553/07.
[148] *Ibid.*, point 70.
[149] *Ibid.*

civile que l'article 7 de la loi du 5 juillet 2016 disposent que « *[t]oute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal* ».

L'infraction prévue à l'article 458 du Code pénal est de nature correctionnelle de sorte que sa prescription est de 5 ans. La Commission nationale est partant d'avis que le délai de conservation des logs files devrait être porté de 12 mois à 5 ans.

D. Quant à l'effacement des résultats

L'article 3, paragraphe 5, du projet de loi précise encore que les informations reçues des opérateurs sont effacées dès confirmation de leur réception par l'autorité judicaire ou le Service de renseignement de l'État et qu'elles ne sont conservées sur la plateforme que le temps nécessaire à la transmission aux autorités requérantes.

Selon le commentaire des articles, ce mécanisme a pour but d'empêcher que la plateforme devienne un « annuaire » de toutes les demandes effectuées dans la mesure où elle ne sert qu'à transmettre les décisions et les résultats.

La Commission nationale se demande pourquoi le projet de loi ne prévoit que l'effacement des résultats transmis par les opérateurs et non pas l'effacement des demandes transmises par les autorités judiciaires ou le Service de renseignement de l'État.

En tout état de cause, l'effacement des résultats de la plateforme ne devrait pas compromettre la vérification de la légalité des opérations effectuées par le biais des logs files.

E. Quant à l'absence de règles de sécurité

Quand bien même le titre du projet de loi contient le terme « sécurisée », il ne prévoit pas, à part le mécanisme des logs files, de règles de sécurité destinées à protéger les traitements de données effectués par le biais de la plateforme.

Certes, l'article 28 de la loi du 1er août 2018 oblige le responsable du traitement et le sous-traitant de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Cependant, cette disposition laisse une marge de manœuvre beaucoup trop grande et n'est pas suffisante au vu du risque que ce traitement présente.

En l'espèce, il faudrait assurer un niveau de sécurité particulièrement élevé. Étant donné que la protection de la vie privée constitue une matière réservée à la loi[150], l'essentiel du cadrage normatif doit figurer dans la loi.

[150] Article 11, paragraphe 3, de la Constitution.

Il paraît dès lors souhaitable de voir compléter le projet de loi par des dispositions relatives aux obligations spécifiques de sécurité en tenant compte de la nature des données et du risque d'atteinte à la vie privée des citoyens.

A cet égard, la Commission nationale entend d'ores et déjà rendre attentifs les auteurs du projet de loi que la mise en place de mesures de sécurité techniques et organisationnelles devrait tenir compte des risques suivants :

- Risque d'interception des messages

  - Identification et authentification systématique de l'émetteur ainsi que du récepteur pour chaque message échangé ;
  - Encryptage du canal de communication ainsi que du message échangé ;
  - Minimisation de tout risque d'écoute de la ligne de communication *(wiretapping)* en considérant en particulier le recours à des lignes non publiques sous contrôle de l'État.

- Risque d'un accès non légitime au système

  - Attribution nominative des accès sur base d'un processus formel et documenté dans le respect rigoureux du principe du *need-to-know need-to-do* ;
  - Revue régulière, systématique et documentée et au moins annuelle de l'ensemble des accès ainsi que des changements d'accès qui ont eu lieu sur la période ;
  - Définition des accès avec un niveau de granularité suffisant pour limiter l'accès à chaque émetteur de message afin de n'avoir accès uniquement qu'au retour de ses propres requêtes ;
  - Accès au système sur base d'une authentification forte ;
  - Accès au système à travers des postes de travail sécurisés et installés dans des locaux sécurisés ;
  - Aucun accès à des données réelles et de manière lisible par le personnel en charge pour développer, opérer, maintenir ou faire évoluer la plateforme ;
  - Sécurité des clé d'encryptage utilisées ;
  - Pertinence et le cas échéant remplacement ou mise à jour des algorithmes d'encryptage utilisés sur la plateforme.

- Risque d'une utilisation illégitime du système

  - Pas de possibilité de reconstruire ou de donner des indications substantielles sur le contenu des messages transmis en utilisant le traçage des opérations techniques et métier *(logs files)* ;

- Pas de possibilité pour les utilisateurs métier ou technique de modifier les logs techniques et métier ;
- Suppression sur les systèmes de l'opérateur des messages (requêtes ou réponses) transmis à l'opérateur ou envoyés par ce dernier dès réception respectivement envoi ;
- Détection d'anomalies ou d'abus métier et techniques à travers des revues régulières systématiques et documentées des logs ;
- Pas d'atteinte par le plan de backup aux durées de rétention des données définies ;
- Formation des utilisateurs ainsi que des opérateurs concernant le fonctionnement et leurs responsabilités spécifiques par rapport à la plateforme;
- Sensibilisation des utilisateurs ainsi que des opérateurs concernant les limites d'utilisation des données, notamment les limites de possibilité de croisement des messages entre eux.

F. <u>Quant à l'obligation d'effectuer une analyse d'impact relative à la protection des données</u>

L'article 26 de la loi du 1er août 2018 prévoit que le responsable du traitement doit effectuer préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques.

Même si les traitements de données effectués par les autorités judiciaires et le Service de renseignement de l'État au titre du projet de loi ne tombent pas dans le champ d'application du RGPD, il y a lieu de noter que ses considérants 92 et 93 disposent ce qui suit :

« Il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée.

Au moment de l'adoption du droit d'un État-membre qui fonde l'exercice des missions de l'autorité publique ou de l'organisme public concernés et qui règlemente l'opération ou l'ensemble d'opérations de traitement spécifiques, les États-membres peuvent estimer qu'une telle analyse est nécessaire préalablement aux activités de traitement. »

Il y a dès lors lieu d'examiner en amont de la mise en place de la plateforme si une analyse d'impact relative à la protection des données s'avère nécessaire ou non.

IV. <u>Modification du Code de procédure pénale et de l'article 7, paragraphe 3, alinéa 1, de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État</u>

Les auteurs du projet de loi expliquent dans l'exposé des motifs que le régime actuellement applicable pose des problèmes de confidentialité considérables en ce que *« la plupart du temps, les OPJ ou les membres du Service de renseignement de l'État notifient les décisions dans un guichet ou local non adapté de l'opérateur qui n'est pas équipé pour garantir la confidentialité nécessaire. Les ordonnances sont répertoriées dans un classeur non autrement sécurisé et se trouvent à la portée d'une bonne partie des employés. La protection des données, la protection de la vie privée et le caractère confidentiel de l'enquête sont dès lors menacées. »*

C'est dans ce souci que la création de la plateforme a comme objectif principal d'améliorer la protection des données à caractère personnel des personnes faisant l'objet de mesures de repérage, de surveillance ou de contrôle.

Comme relevé au point III. E du présent avis, la Commission nationale n'est actuellement pas en mesure de l'apprécier, faute de plus amples précisions dans le projet de loi. Dans ce contexte, elle se pose par ailleurs la question de savoir pourquoi, au regard des déficiences du système actuel et des avantages de la plateforme mis en avant dans l'exposé des motifs, le projet de loi ne rend pas le recours à cette plateforme obligatoire.

Selon l'exposé des motifs, le projet de loi ne compte pas faire de la notification par voie électronique moyennant la plateforme commune une obligation. Cela est corroboré par les articles 4 et 5 du projet de loi selon lesquels *« [l]es éléments et informations techniques nécessaires (…) sont communiqués [notifiés] y compris par voie électronique sécurisée au travers de la plateforme (…) »*.

S'il ressort clairement du projet de loi que la transmission par les autorités judiciaires et le Service de renseignement de l'État aux opérateurs peut également se faire par d'autres moyens, il semble toutefois que les opérateurs soient obligés de transmettre les résultats au travers de la plateforme, tout au moins en ce qui concerne l'article 67-1 du Code de procédure pénale et l'article 7, paragraphe 3, de la loi du 5 juillet 2016.

En effet, le projet de loi prévoit de modifier le paragraphe 2 de l'article 67-1 en ce sens qu'il disposera que les opérateurs de télécommunications et les fournisseurs d'un service de télécommunications *« transmettent les résultats de cette exécution au moyen de la même plateforme dans les meilleurs délais », sans faire de distinction selon le moyen par lequel la requête leur est parvenue.*

En ce qui concerne l'article 7, paragraphe 3, de la loi du 5 juillet 2016, se pose également la question de savoir si les résultats doivent être transmis obligatoirement par la plateforme, peu importe le moyen par lequel la requête a été adressée, ou s'il y a lieu de suivre un « parallélisme des formes ».

L'article 88-4, paragraphe 1, du Code de procédure pénale, tel que modifié par le projet de loi, ne contient par contre aucune indication quant au moyen par lequel les résultats sont à transmettre. Il est simplement mentionné que chaque *« opérateur des postes et télécommunications »* tient un registre spécial dans lequel sont inscrits les éléments et les informations techniques notifiés et les suites qui leur sont données.

Au regard des fortes réserves que les auteurs du projet de loi ont exprimé à l'égard des « classeurs » tenus actuellement par les opérateurs et répertoriant les ordonnances, la Commission nationale s'interroge sur l'utilité de ce registre spécial. De plus, le projet de loi ne contient pas d'explications quant à l'utilisation du terme « opérateur des postes et télécommunications ». A cet égard, la Commission nationale se permet de renvoyer à ses développements sous le point II. du présent avis.

L'article 88, paragraphe 3, du Code de procédure pénale reste inchangé en ce qu'il prévoit que *« [l]es télécommunications, correspondances postales, images, conversations ou données enregistrées ou interceptées sont remises sous scellés et contre récépissé au juge d'instruction qui dresse procès-verbal de leur remise »*.

La Commission nationale se pose la question de savoir comment cette disposition s'articule avec la transmission électronique au travers de la plateforme telle que prévue par le projet de loi.

Par ailleurs, il n'est pas clair pour la Commission nationale de quelle manière s'opérera la transmission, par le biais de la plateforme, des résultats de la surveillance et du contrôle de « correspondance postale » visée dans le prédit article 88, paragraphe 3, du Code de procédure pénale.

En outre, l'article 7, paragraphe 1, de la loi du 5 juillet 2016 vise la surveillance et le contrôle de la communication électronique et de la « correspondance postale ».

Le paragraphe 3, alinéa 1, dudit article, tel que modifié par le projet de loi, ne mentionne toutefois que la transmission des éléments et information techniques nécessaires à l'exécution des mesures de surveillance et de contrôle aux opérateurs de « télécommunications » et aux fournisseurs d'un service de « télécommunications ». Il n'est pas clair pour la Commission nationale par quel biais les requêtes concernant la surveillance et le contrôle de la « correspondance postale » seront transmises aux opérateurs concernés[151], respectivement de quelle manière les résultats sont à transmettre.

[151] La même remarque vaut pour l'article 88-4 du Code de procédure pénale.

De plus, l'article 7, paragraphe 3, alinéa 3, de la loi du 5 juillet 2016 reste inchangé en ce qu'il dispose que *« [l]es correspondances sont mises sous scellés et remises contre récépissé au SRE, qui fait copier les correspondances pouvant servir à ses investigations et renvoie les écrits qu'il ne juge pas nécessaire de retenir aux opérateurs qui les font remettre au destinataire ».*

La Commission nationale s'interroge sur l'articulation de cette disposition avec la transmission électronique au travers de la plateforme telle que prévue par le projet de loi.

Ainsi décidé à Esch-sur-Alzette en date du 5 juin 2019.

La Commission nationale pour la protection des données,

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

Avis de la Commission nationale pour la protection des données relatif :
1. au projet de loi n°6054 sur les associations sans but lucratif et les fondations ;
2. à la proposition de loi n°7392 portant modification de la loi modifiée du 21 avril 1928 sur les associations et les fondations sans but lucratif.

Délibération n°41/2019 du 18 juin 2019

Conformément à l'article 57 paragraphe (1) lettre (c) du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après désigné « le RGPD »), chaque autorité de contrôle a pour mission de conseiller *« conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement »*. L'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

A ce titre, la Commission nationale s'autosaisie pour aviser le projet de loi n°6054 sur les associations sans but lucratif et les fondations, ainsi que la proposition de loi n°7392 portant modification de la loi modifiée du 21 avril 1928 sur les associations et les fondations sans but lucratif.

1. Le contexte de l'auto-saisine de la CNPD

1.1. L'obligation de dépôt et l'obligation de publication de documents d'une association

A titre préliminaire, la CNPD rappelle que les associations sans but lucratif (ci-après : « l'association » ou « les associations ») sont obligées de par la loi à accomplir certaines formalités administratives. La loi modifiée du 9 décembre 2002 concernant le registre de commerce et des sociétés, ainsi que la comptabilité et les comptes annuels des entreprises, opère dans ce contexte une distinction entre l'obligation de dépôt de documents auprès du registre de commerce et des sociétés (ci-après: « RCS ») d'un côté et l'obligation de publication de documents au recueil électronique des sociétés et associations (ci-après : « RESA ») d'autre côté. Le Luxembourg Business Registers (« LBR »), un groupement d'intérêt économique comprenant l'État, la Chambre de Commerce et la Chambre des Métiers, assure sous la tutelle du ministre de la Justice la gestion du RSC, du RESA, ainsi que du Registre des bénéficiaires effectifs (« RBE »).

ANNEXES

5

La loi modifiée du 21 avril 1928 sur les associations et les fondations sans but lucratif (ci-après : « la loi modifiée du 21 avril 1928 ») précise quels documents d'une association doivent faire l'objet d'une publication au RESA, comme par exemple l'acte constitutif. Le RESA est la plateforme électronique centrale de publication officielle au Luxembourg, qui remplace depuis le 1er juin 2016 le Mémorial C. Les documents y publiés sont accessibles par chaque internaute sans démarches supplémentaires.

Le dépôt de documents par une association par contre consiste en la remise au RCS de documents soumis à l'obligation de dépôt de par la loi modifiée du 21 avril 1928 en vue de leur classement dans le dossier de l'association tenu par le gestionnaire du RCS. Néanmoins, en recherchant sur le portail du RCS une association précise, la majorité des documents déposés par cette dernière peuvent être téléchargés sans frais par toute personne ayant mis en place un compte utilisateur auprès du RCS. Lors de la création dudit compte, il est uniquement obligatoire d'indiquer son nom et prénom, une adresse e-mail, le nom d'utilisateur souhaité, ainsi qu'un mot de passe.

1.2. L'obligation spécifique de déposer une liste des membres d'une association

L'auto-saisine de la CNPD intervient dans le cadre de nombreuses demandes d'information et de réclamations introduites auprès d'elle concernant le dépôt auprès du RCS d'un document spécifique contenant un certain nombre de données à caractère personnel des membres d'une association. Plus concrètement, l'article 10 de la loi modifiée du 21 avril 1928 prévoit qu'une *« liste indiquant, par ordre alphabétique, les noms, prénoms, demeures et nationalités des membres de l'association, doit être déposée auprès du registre de commerce et des sociétés dans le mois de la publication des statuts »* et que *« toute personne pourra en prendre gratuitement connaissance. »*

Une association en sa qualité de responsable du traitement est de ce fait obligée sur base de l'article 10 de la loi modifiée du 21 avril 1928 de transmettre les données y mentionnées au RCS, c'est-à-dire l'association doit a priori baser ce traitement de données sur le respect d'une obligation légale à laquelle le responsable du traitement est soumis (article 6 paragraphe (1) lettre c) du RGPD). Comme susmentionné, par la création d'un compte utilisateur et en recherchant une association déterminée, toute personne qui le souhaite peut télécharger une copie de la majorité des documents soumis au dépôt par ladite association auprès du RCS. La liste des membres d'une association fait partie de ces documents téléchargeables.

Par ailleurs et indépendamment sur lequel des six critères de licéité prévus à l'article 6 paragraphe (1) du RGPD un traitement est basé, les principes de limitation des finalités et de minimisation des données prévus par l'article 5 paragraphe (1) lettres b) et c) du RGPD sont à respecter, ceux-ci exigeant qu'uniquement des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités légitimes sont collectées.

1.3. La problématique générale soulevée par le dépôt de la liste des membres

De manière générale, la CNPD comprend la nécessité de tenir une liste des membres à des fins de gestion administrative interne d'une association, incluant certaines données à caractère personnel comme le nom, prénom et une adresse postale / mail des différents membres. En plus, comme l'appartenance à une association peut dans certains cas et en fonction des statuts et des activités poursuivies être considérée comme relation contractuelle entre les membres et l'association elle-même, la CNPD considère que les différents membres ont le droit de connaître l'identité de leurs co-contractants.

Néanmoins, en tenant compte de l'évolution de la liberté d'association depuis l'adoption de la loi modifiée du 21 avril 1928, la Commission nationale se demande en quoi consiste de nos jours la finalité d'accorder un accès à la liste des membres d'une association à des tiers. Comme susmentionné, sous condition de respecter certaines formalités administratives, des personnes étrangères à une association peuvent en effet avoir accès à la liste des membres en la téléchargeant sur le portail du RCS. D'autant plus, la simple consultation d'une liste des membres d'une association peut constituer un traitement portant sur des catégories particulières de données à caractère personnel, données dites « sensibles », dans la mesure où le fait d'être membre de certaines associations peut par exemple révéler les convictions religieuses, l'appartenance syndicale, les opinions politiques, l'orientation sexuelle des membres, etc. Rappelons que le traitement de ces données est très strictement encadré par l'article 9 du RGPD.

La CNPD est bien consciente que l'adoption de loi modifiée du 21 avril 1928 est largement antérieure à l'entrée en application du RGPD, ce qui explique certains conflits entre les deux textes. L'article 10 de ladite loi faisait d'ailleurs partie de la version initiale de 1928, avec la seule différence que le dépôt de la liste des membres d'une association devrait s'effectuer auprès du greffe du tribunal civil du siège de l'association et non pas auprès du RCS (non existant à l'époque). Par ailleurs, l'article 10 précité prévoyait déjà en 1928 que toute personne pourrait *« prendre gratuitement connaissance »* de la liste des membres d'une association. La CNPD considère que l'article 10 en question, vieux de plus de 90 ans, mérite d'être adapté aux exigences du RGPD pour tenir compte du fait que ces consultations peuvent entretemps se faire par n'importe qui, de manière électronique à partir de n'importe où, et le cas échéant en grande quantité. A ce titre, elle ne peut que partager l'avis de la Chambre des salariés à cet égard, ayant énoncé de manière pertinente dans son avis du 7 mai 2019 concernant la proposition de loi n°7392 portant modification de loi modifiée du 21 avril 1928 sur les associations et fondations sans but lucratif ce qui suit :

« Vu l'origine de la disposition de l'article 10 qui date de 1928 et qu'elle ne fût jamais adaptée aux nouvelles exigences et tendances dans le domaine de la protection des données, on peut considérer que lors de l'entrée en vigueur de la disposition, celle-ci ne prévoyait pas encore les moyens modernes de mise en relation de plusieurs sources de données afin d'établir des liens et des corrélations. Combinant ceci avec la disponibilité des données en question par internet, il semble que le traitement en question devrait être repensé en prenant compte les avancées récentes dans le domaine de la protection des données. »

La CNPD tient donc à développer ci-dessous son point de vue sur le projet de loi n°6054 sur les associations sans but lucratif et les fondations, ainsi que sur la proposition de loi n°7392 portant modification de la loi modifiée du 21 avril 1928 sur les associations et les fondations sans but lucratif.

2. <u>Quant au projet de loi n°6054 sur les associations sans but lucratif et les fondations</u>

Déjà en date du 10 juin 2009, l'ancien Ministre de la Justice, Monsieur Luc Frieden, avait déposé le projet de loi n°6054 sur les associations sans but lucratif et les fondations (ci-après: « le projet de loi n°6054 »), prévoyant de réformer tout le système légal applicable en la matière en abrogeant la loi modifiée du 21 avril 1928. Or, le projet de loi n'a pas connu de suites pendant 5 ans et ce n'est que le 13 décembre 2018 qu'il a été renvoyé de nouveau à la Commission de la Justice de la Chambre des députés.

A ce stade, la Commission nationale n'entend pas commenter le projet de loi n°6054 dans son ensemble, alors que ledit projet de loi fera encore l'objet d'amendements ultérieurs et qu'elle sera saisie pour avis le moment venu. Néanmoins, elle tient d'ores et déjà à se prononcer sur l'article 9 du projet de loi n°6054 qui prévoit que le conseil d'administration tient au siège de l'association un registre des membres comprenant *« les nom, prénoms et l'adresse privée ou professionnelle précise des membres, ou lorsqu'il s'agit d'une personne morale, la dénomination sociale, la forme juridique, l'adresse du siège social ainsi que le numéro d'immatriculation au registre de commerce et des sociétés. »* Cet article en projet ne prévoit donc plus la publication des données des membres d'une association accessibles à tout le monde. En effet, il ressort du paragraphe (3) de l'article 9 du projet de loi n°6054 qu'uniquement les membres de l'association ont la possibilité de consulter au siège de l'association, entre autres, le registre précité des membres. Par ailleurs, ledit paragraphe précise que les « documents et pièces » y mentionnés, dont le registre des membres, « ne pourront pas être déplacés ».

Selon le commentaire des articles, l'article 9 vise précisément à *« remplacer l'obligation de déposer une liste des membres au registre de commerce et des sociétés, telle qu'elle résulte de l'article 10 de la loi de 1928, par l'obligation de tenir un registre des membres au siège de l'association. […] Grâce à l'institution de pareil registre, tous les membres de l'association pourront désormais en consulter le contenu à tout moment au siège de l'association en vue de connaître avec précision l'identité des membres de l'association. Ils n'auront plus besoin de consulter la liste déposée au registre de commerce et des sociétés en vue d'obtenir cette information. »* Les seules données à caractère personnel relatives aux membres et accessibles à des tiers par la publication des statuts au RESA concernent uniquement les membres-fondateur d'une association. En effet, selon l'article 3 paragraphe (1) point 4 du projet de loi n°6054, les statuts doivent mentionner les nom, prénoms et l'adresse privée ou professionnelle précise des membres-fondateur de l'association.

La Commission nationale ne peut que saluer le projet de loi n°6054 en ce qu'il supprime l'obligation de dépôt de la liste des membres d'une association auprès du RCS, consultable par des tiers dans les conditions susmentionnées

sous les points 1.1. et 1.2. du présent avis, et qu'il la remplace par la tenue d'une telle liste au sein du siège de l'association consultable uniquement par ses membres. Comme l'a constaté la Chambre des salariés dans son avis précité du 7 mai 2019 : *« il s'agit de rétablir, du fait du développement fulgurant des réseaux électroniques, l'équilibre entre les données qui sont vraiment indispensables pour l'intérêt général et l'ordre public, à savoir l'identité des membres composant le conseil d'administration d'une asbl et la protection des données des membres qui la composent et, par-là, leur vie privée afin d'éviter toute curiosité malsaine susceptible de leur porter préjudice. »*

Un dernier doute subsiste cependant en ce qui concerne l'obligation imposée à chaque association de tenir un registre des membres à son siège, alors que les auteurs énoncent dans l'exposé des motifs du projet de loi n°6054 que ledit registre *« peut être consulté par tous les membres (et les tiers). »* Or, la CNPD avait compris que cette obligation de tenir un registre des membres au siège de l'association avait précisément comme but de ne plus le rendre accessible au public en général ou à des « tiers », c'est-à-dire à des personnes extérieures à l'association. A titre de comparaison, la loi belge modifiée du 27 juin 1921 sur les associations sans but lucratif, les fondations, les partis politiques européens et les fondations politiques européennes limite strictement l'accès aux données des membres d'une association. Le texte belge précise en effet qu'en dehors des membres de l'association, cette dernière doit uniquement, *« en cas de requête orale ou écrite, accorder immédiatement l'accès au registre des membres aux autorités, administrations et services, y compris les parquets, les greffes et les membres des cours, des tribunaux et de toutes les juridictions et les fonctionnaires légalement habilités à cet effet […]. »* Ainsi, à l'instar du texte belge, la CNPD suggère aux auteurs du projet de loi de limiter précisément dans le corps du texte quels sont les destinataires potentiels du registre des membres.

3. Quant à la proposition de loi n°7392 portant modification de la loi modifiée du 21 avril 1928 sur les associations et les fondations sans but lucratif

En date du 18 décembre 2018, la proposition de loi n°7392 portant modification de la loi modifiée du 21 avril 1928 sur les associations et les fondations sans but lucratif (ci-après: « la proposition de loi n°7392 ») a été déposée par les députés Sven Clement et Marc Goergen. Ladite proposition de loi a été déclarée recevable et renvoyée en Commission de la Justice en date du 29 janvier 2019. Suite à l'entrée en application du RGPD le 25 mai 2018, les auteurs de la proposition de loi s'interrogent précisément *« sur la nécessité et la finalité de la publication de données à caractère personnelle accessible par internet de chaque membre d'une association sans but lucratif. »* Par son article unique, la proposition de loi n°7392 vise à modifier l'article 10 de la loi modifiée du 21 avril 1928 en remplaçant l'obligation de déposer une liste des membres au RCS par la tenue d'une *« liste indiquant, par ordre alphabétique, les noms, prénoms, demeures et nationalités des membres de l'association »*. Similairement au projet de loi n°6054, la proposition de loi prévoit que ladite liste doit être tenue par les administrateurs au siège de l'association et que chaque membre de l'association pourra en prendre gratuitement connaissance.

De manière générale, la Commission nationale salue également la proposition de loi n°7392 prévoyant de remplacer l'obligation de dépôt de la liste des membres d'une association auprès du RCS, consultable par des tiers dans les conditions susmentionnées sous les point 1.1. et 1.2. du présent avis, par la tenue d'une telle liste au sein du siège de l'association consultable uniquement par ses membres. Au regard des principes prévus à l'article 5 du RGPD, la CNPD s'interroge cependant sur la finalité et la nécessité de collecter et de traiter la nationalité des membres d'une association. A ce titre, elle a une nette préférence pour le texte du projet de loi n°6054 qui ne prévoit pas l'obligation de mentionner la nationalité.

4. Conclusion

Selon les principes de limitation des finalités, ainsi que de minimisation des données, les données à caractère personnel traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire pour atteindre les finalités légitimes qui ont été déterminées lors de la collecte des données à caractère personnel (article 5 paragraphe (1) lettres b) et c) du RGPD). En fonction des finalités spécifiques ainsi déterminées et à l'égard du principe de nécessité et de proportionnalité, le responsable du traitement doit ainsi déterminer quelles données à caractère personnel peuvent être utilisées pour atteindre les différentes finalités. Le considérant 39 du RGPD précise à cet égard que les *« données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens. »*

Alors que la CNPD estime qu'il est raisonnable de tenir une liste des membres d'une association à des fins de gestion administrative interne et consultable précisément par lesdits membres, elle s'interroge sur la finalité poursuivie par le fait de rendre accessible cette liste à des tiers.

Ainsi, la Commission nationale est d'avis qu'il existe actuellement une contradiction entre l'article 10 de loi modifiée du 21 avril 1928 et le respect de la vie privée des membres d'une association, ainsi que la protection de leurs données à caractère personnel au regard du RGPD et pour cette raison, elle salue les deux initiatives législatives. Par ailleurs, comme le montrent les réclamations et demandes d'informations reçues par la CNPD, les associations se retrouvent momentanément dans une situation juridique incertaine, entre l'obligation de déposer la liste des leurs membres auprès du RCS, résultant d'une loi nationale vieille de 90 ans, d'un côté et le respect des dispositions du RGPD, norme législative supérieure, d'autre côté. Afin de parer à cette insécurité juridique et d'assurer la conformité du cadre légal luxembourgeois au RGPD, la CNDP estime donc nécessaire de procéder rapidement à la modification de l'article 10 de la loi modifiée du 21 avril 1928. En effet, la CJUE exige des États-membres de l'Union européenne de mettre en conformité leurs législations et leurs réglementations nationales existantes avec les règlements européens, en jugeant que *« la primauté et l'effet direct des dispositions du droit communautaire ne dispensent pas les États-membres de l'obligation d'éliminer de leur ordre juridique interne les dispositions incompatibles avec le droit communautaire; en effet, leur maintien engendre une situation de fait ambiguë, en laissant les sujets de droit concernés dans un état d'incertitude quant aux possibilités qui leur sont réservées de faire appel au droit communautaire.»*

Ainsi décidé à Esch-sur-Alzette en date du 18 juin 2019.

La Commission nationale pour la protection des données

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

ANNEXES

5

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

Délibération n°42/2019 du 8 juillet 2019

Conformément à l'article 57, paragraphe 1er, lettre (c) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

Par courrier en date du 15 mars 2019, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer sur le projet de loi n°7425 portant : 1° transposition de la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes ; 2° modification du Code pénal, et 3° abrogation de la loi du 20 avril 1881 concernant le transport et le commerce des matières explosives (ci-après le « projet de loi »).

Ledit projet de loi a pour objet de transposer en droit national la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes (ci-après la « directive »).

Selon l'exposé des motifs, ce projet de loi entend procéder à une refonte complète de la loi modifiée du 15 mars 1983 sur les armes et munitions (ci-après la « loi modifiée du 15 mars 1983), en outre celui-ci *« prévoit concernant ses aspects les plus importants, des dispositions relatives :*
1° à une meilleure définition et classification des armes ;
2° à l'interdiction de certaines armes semi-automatiques considérées comme étant particulièrement dangereuses ;
3° à l'introduction de la neutralisation d'armes à feu ;
4° à l'exigence d'une attestation médicale ;

5° à une interdiction de manipuler des armes sous l'emprise de l'alcool ;
6° au stockage des armes ;
7° aux exportations d'armes ;
8° au renforcement des mesures de contrôle de l'application de la future loi, et
9° au renforcement des dispositions pénales en la matière. »

Dans la mesure où le présent projet de loi transpose en droit national la directive précitée, la Commission nationale renvoie en ce qui concerne le cadre légal de cette directive à l'avis du 17 février 2014 du Contrôleur européen de la protection des données (ci-après le « CEPD ») sur *« Les armes à feu et la sécurité intérieure dans l'Union européenne : protéger les citoyens et déjouer les trafics illicites »* et limitera ses observations aux dispositions légales concernant la mise en œuvre concrète de cette directive au Luxembourg.

Le présent avis traitera donc des questions relatives aux aspects de la protection des données à caractère personnel, soulevées par les articles 13 (Fichier des armes et traitement de données à caractère personnel), 14 (Attestation médicale), 15 (Agrément d'armurier et de commerçant d'armes), 17 (Salariés et collaborateurs des armuriers), 19 (Registre d'armes), 22 (Conditions générales concernant l'octroi des autorisations aux particuliers) et 52 (Contrôles effectués par l'Administration des douanes et accises) du projet de loi.

I. <u>Remarques préliminaires</u>

Tout d'abord, il convient de relever que, dans la mesure où le présent projet de loi constitue une refonte complète de la loi modifiée du 15 mars 1983, certains éléments qui figurent dans le projet de loi ne découlent pas directement de la directive mais sont utiles et nécessaires pour encadrer les différents traitements mis en œuvre par le Ministre ayant dans ses compétences la loi sous avis (ci-après le « ministre »).

Du fait de l'abrogation de la loi modifiée du 15 mars 1983, la CNPD comprend que le *« fichier des armes prohibées et autorisations »*, visé par l'article 5, alinéa 4, de la loi précitée, sera remplacé par le *« fichier des armes »* créé par l'article 13 du projet de loi. D'un point de vue du principe de la sécurité juridique, la Commission nationale salue que le principe de la création d'un tel fichier soit prévu par le projet de loi conformément à l'article 6, paragraphe (3) du RGPD[152]. Cet article prévoit, en effet, une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans ces deux cas de figure, le fondement et les finalités des traitements de données doivent spécifiquement être prévus soit par le droit de l'Union européenne, soit par le droit de l'État-membre auquel le responsable du traitement est soumis.

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

[152] L'article 6, paragraphe (3) dispose que la *« base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du règlement, entre autres : les conditions générales régissant la licéité du traitement par le responsable du traitement ; les personnes concernées ; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ; la limitation des finalités ; les durées de conservation ; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX ».*

générales du présent règlement régissant la licéité du traitement des données à caractère personnel, établir les spécifications visant à déterminer le responsable du traitement, le type de données à caractère personnel faisant l'objet du traitement, les personnes concernées, les entités auxquelles les données à caractère personnel peuvent être communiquées, les limitations de la finalité, la durée de conservation et d'autres mesures visant à garantir un traitement licite et loyal. […] ». En vertu des dispositions précitées, ces bases légales devraient contenir des dispositions spécifiques concernant, entre autres, les types de données traitées, les personnes concernées, les entités auxquelles les données peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

Toutefois et bien que le principe de la création d'un tel fichier soit prévu dans le projet de loi, la Commission relève que certains éléments relatifs au traitement de données ne sont pas (ou pas suffisamment) précisés dans le projet de loi.

En outre, la Commission nationale constate à la lecture du projet de loi qu'il est fait référence au *« fichier des armes prohibées »* à l'article 52 du projet de loi. Les auteurs du projet de loi mentionnent encore un *« fichier du Service des armes prohibées »* dans le commentaire de l'article 19 du projet de loi. Dans ce contexte, la Commission se demande s'il existe plusieurs fichiers ou s'il s'agit du fichier qui est visé à l'article 13 du projet de loi. Dans une telle hypothèse, ne conviendrait-il pas dans un souci de clarté et pour une meilleure compréhension desdits articles, de renvoyer expressément au fichier visé à l'article 13 ou d'utiliser la même terminologie à savoir le *« fichier des armes »* ? A contrario, s'il s'agit de fichiers différents, il conviendrait alors de l'indiquer expressément dans le projet de loi, et de préciser pour chacun de ces fichiers les finalités, catégories de données, etc. qui y sont associées.

Il ressort des développements qui précèdent que la Commission nationale ne dispose pas de toutes les informations concernant l'ensemble des traitements de données à caractère personnel mis en œuvre dans le cadre du projet de loi et ne peut pas apprécier pleinement si les traitements mis en œuvre sont conformes au RGPD.

La CNPD précisera, dès lors, dans les développements ci-après, les éléments manquants concernant les traitements effectués dans le cadre de la tenue du fichier visé à l'article 13 (II), les spécificités relatives au traitement de données relatives aux infractions pénales et à la santé qui doivent être respectées par le responsable du traitement (III), les clarifications devant être apportées au registre des armes tenus par les armuriers (IV) et à l'accès prévu par l'article 52 du projet de loi pour les agents de l'Administration des douanes et accises (V).

II. Sur le « fichier comportant les données à caractère personnel » visé à l'article 13 du projet de loi

Comme indiqué précédemment, la Commission nationale comprend que ce fichier a vocation à remplacer le « fichier des armes prohibées et autorisations » visé par l'article 5, alinéa 4, de la loi modifiée du 15 mars 1983 (ci-après le *« fichier des armes prohibées et autorisations »*).

1. <u>Sur la base juridique sur laquelle se fonde le traitement</u>

En premier lieu, il convient de rappeler qu'un traitement de données à caractère personnel n'est licite que si au moins une des conditions visées à l'article 6, paragraphe (1) lettres a) à f) est remplie.

Il ressort du paragraphe (4) de l'article 13 du projet de loi, que les auteurs du projet de loi entendent fonder le traitement de données, tel que visé à l'article 13 précité, sur le consentement des personnes concernées.

Or, il convient de relever que d'une part la rédaction actuelle de l'article ne permet pas de recueillir un consentement valable au sens du RGPD et d'autre part cette base de licéité n'est pas la plus appropriée dans le cadre de la présente loi sous avis.

Concernant le consentement de la personne concernée, il convient de rappeler que conformément à l'article 4, paragraphe (11) du RGPD, le consentement est défini 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 »*. Toutefois, la formulation actuelle du paragraphe (4) de l'article 13 du projet de loi en ce qu'il dispose que *« la personne concernée consent au traitement de ses données personnelles, y compris à ce que le bulletin n°2 du casier judiciaire soit délivré directement par le procureur général d'État au Ministre. »*, n'est pas conforme au sens du RGPD, en ce que le consentement donné par la personne concernée s'apparente à un consentement forcé.

En effet, il convient de rappeler que l'un des éléments d'un consentement valable est une *« manifestation de volonté libre »*. L'adjectif *« libre »* implique un choix et un contrôle réel pour les personnes concernées. Ainsi, si la personne concernée n'est pas véritablement en mesure d'exercer un choix, se sent contrainte de consentir ou subira des conséquences négatives importantes si elle ne donne pas son consentement, alors le consentement ne sera pas valable[153].

En tout état de cause, le considérant 43 du RGPD indique clairement qu' *« il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. »*. De plus, le Groupe de travail « Article 29 » considère encore, dans ses lignes directrices sur le consentement au sens du RGPD[154], qu'il existe d'autres bases juridiques en principe plus appropriées aux activités des autorités publiques, notamment le paragraphe (1), points c) et e) de l'article 6 du RGPD.

Au vu de ce qui précède, la Commission suggère donc que le passage suivant « la personne concernée consent au traitement de ses données à caractère personnel » soit supprimé.

[153] Page 6 des lignes directrices sur le consentement au sens du RGPD, Groupe de travail « Article 29 », adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2018.
[154] Point 3.1.1. Déséquilibre des rapports de force, pages 6 et 7 des lignes directrices sur le consentement au sens du RGPD, Groupe de travail « Article 29 », adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2018.

2. Sur la détermination des finalités du traitement

Tout d'abord, il convient de rappeler que conformément à l'article 5 paragraphe (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, l'article 6 paragraphe (3) du RGPD, lu ensemble avec son paragraphe (1) lettre c) et (e), prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans ces deux cas de figure, le fondement et les finalités des traitements de données doivent spécifiquement être prévus soit par le droit de l'Union européenne, soit par le droit de l'État-membre auquel le responsable du traitement est soumis.

Le considérant (41) du RGPD précise encore que *« cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne* (ci-après dénommée « Cour de justice ») *et de la Cour européenne des droits de l'homme. »*

Au vu de ce qui précède, la Commission nationale estime que la finalité telle qu'actuellement rédigée au paragraphe (1) de l'article 13 : « (…) le traitement est nécessaire aux fins de l'exécution de la présente loi » est formulée de manière trop vague.

Compte tenu des développements précédents, la Commission nationale recommande dès lors de préciser les finalités des traitements et se demande s'il ne serait pas plus pertinent de transposer à l'identique le paragraphe (4) alinéa premier de l'article 4 de la directive qui précise que : *« Ce fichier de données comprend toutes les informations relatives aux armes à feu qui sont nécessaires pour tracer et identifier ces armes à feu ».*

Toutefois, si le fichier visé à l'article 13 du projet de loi traite également des données pour d'autres finalités, alors cet article devra être complété et préciser ces autres finalités. En effet, la CNPD se demande si le ministre ne collecterait pas des données à caractère personnel à des fins de gestion administrative des autorisations pour le port d'armes. Sur ce point, la Commission nationale souhaite attirer l'attention sur les dispositions légales prévues par le législateur belge qui a précisé concernant le registre central des armes, que les informations contenues dans ce fichier ne peuvent être utilisées que pour *« la gestion des documents prévus à l'article 29, et dans le cadre des missions de police judiciaire et administrative de ces autorités et services »*[155].

Conformément au principe de la limitation des finalités, les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. En principe, les données ne doivent pas être traitées pour des finalités « incompatibles » avec

[155] Article 28 de l'arrêté royal exécutant la loi sur les armes du 20 septembre 1991, tel que modifié.

ces finalités initiales précisées dans la loi. Il conviendrait donc si le fichier concerne plusieurs finalités d'indiquer précisément quelles catégories de données sont traitées pour quelles finalités.

3. Sur les catégories de données à caractère personnel

Par ailleurs, la Commission nationale se félicite de la précision des catégories de données à caractère personnel, telles qu'énumérées au paragraphe (2) de l'article 13 du projet de loi qui est d'ailleurs une reprise littérale de la liste qui figure à l'article 4 paragraphe (4) de la directive.

Toutefois, la Commission a constaté qu'afin de délivrer des autorisations administratives concernant les armes à feu, le ministre est actuellement amené à collecter et traiter des données personnelles telles que les photos d'identité, la copie de la carte d'identité du demandeur d'un permis d'arme ainsi que le cas échéant la copie de la carte d'identité du vendeur de l'arme. Ces documents sont, en effet, listés dans les annexes à joindre à la demande en obtention d'un permis d'armes, tel que cela figure sur le formulaire *« Première demande en obtention d'un permis d'armes »*[156]. Or, la collecte de ces catégories de données à caractère personnel n'est pas précisée dans le texte du projet de loi.

Si l'intention du ministère ayant la justice dans ses attributions est de continuer à collecter de telles données dans le cadre de la délivrance de telles autorisations, la CNPD estime indispensable que ces catégories de données soient également clairement détaillées dans le projet de loi, et recommande d'énumérer quelles données sont collectées et pour quelles finalités. Il est, en effet, difficile de comprendre à la lecture du projet de loi quel est réellement l'ensemble des données qui sont collectées par le ministre, et à quelles fins celles-ci sont traitées.

4. Sur les personnes concernées

La Commission nationale recommande que le législateur insère des dispositions concernant les catégories de personnes concernées (acquéreur, fournisseur, titulaire d'une autorisation de détention d'armes…) pour les différents traitements susceptibles d'être mis en œuvre dans le cadre du présent projet de loi. En effet, il conviendrait de préciser quelles catégories de personnes sont concernées par ces traitements, et d'indiquer quelles sont les catégories de données qui s'y rapportent.

5. Sur l'origine des données à caractère personnel

La Commission nationale constate que l'origine des données traitées par le ministre n'est pas précisée dans le texte de l'article 13 du projet de loi. Une clarification à ce titre mériterait d'être précisée. Est-ce que les données sont collectées à partir des formulaires devant être remplis par les personnes qui souhaitent obtenir un permis d'armes ? Existe-il d'autres sources qui permettraient au Ministère de collecter indirectement les données relatives

[156] Disponible sur le site du Ministère de la Justice à l'adresse suivante : https://guichet.public.lu/fr/formulaires/armes/obtention-permis-arme.html

aux fournisseurs, acquéreurs ou détenteurs d'armes au Luxembourg à partir d'autres fichiers étatiques ? Dans l'affirmative, une telle communication de données entre ministères ou administrations devraient être précisée dans le texte du projet de loi.

6. Sur l'accès aux données à caractère personnel

La Commission nationale regrette le manque de précision dans l'article 13 du projet de loi quant à l'accès aux données.

i. Sur l'accès aux données à caractère personnel par le ministre et ses agents

La CNPD recommande de préciser qu'au sein du Ministère de la Justice l'accès aux données soit limité aux seuls agents ayant besoin d'en connaître dans le cadre de leur fonction. Il conviendrait également de prévoir les modalités de cet accès et de mettre en place une procédure comportant des garanties appropriées visant à exclure toute utilisation allant au-delà des finalités pour lesquelles ces données sont initialement traitées.

ii. Sur l'accès aux données par les « autres autorités compétentes administratives »

La Commission nationale regrette que le point 1) du paragraphe (3) de l'article 13 du projet de loi contient une formulation vague. Cet article prévoit, en effet, que l'accès aux données à caractère personnel visées au paragraphe (2) de l'article 13 est accessible à *« d'autres autorités compétentes administratives qui ont besoin d'en connaître dans l'exercice de leurs missions légales pendant une période maximale de dix ans qui court à partir de la destruction de l'arme à feu ou des parties essentielles en question »*.

Or, cette formulation vague ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal. Une loi doit être suffisamment claire et précise afin de permettre aux personnes concernées de connaître l'étendue des limitations, ainsi que les conséquences éventuelles pour elles[157].

Par ailleurs, il convient de noter que l'article 4 paragraphe (4), alinéa 2, de la directive, que la disposition sous avis est appelée à transposer, est plus précis en ce qu'il dispose que : *« les données à caractère personnel y afférentes sont accessibles : a) aux autorités compétentes afin d'accorder ou de retirer les autorisations visées à l'article 6 ou 7 ou aux autorités compétentes en matière de procédure douanière, pendant une période de dix ans après la destruction de l'arme à feu ou des parties essentielles en question »*. Il ressort de ce qui précède que la formulation retenue par les auteurs du projet de loi élargit le nombre d'autorités visées par l'article 4 paragraphe (4), alinéa 2, de la directive. En ne suivant pas la directive sur ce point, le projet de loi sous avis procède à une transposition incorrecte de la directive. La CNPD est d'avis que les auteurs du projet de loi doivent préciser la disposition, c'est-à-dire énumérer les autorités visées mais ne peuvent pas aller au-delà de ce qui est prévu par la directive.

[157] Voir entre autres CourEDH, Zakharov c. Russie [GC], n°47413/06, § 228-229, 4 décembre 2015.

La Commission estime, dès lors, nécessaire d'énumérer les autorités administratives susceptibles d'y avoir accès et de préciser qu'un tel accès sera limité aux collaborateurs de l'autorité / l'organe ayant besoin d'en connaître. De plus et comme indiqué au point ci-avant, cet accès aux données ne doit pas permettre une utilisation qui diffère des finalités pour lesquelles ces données sont traitées.

iii. Sur la traçabilité des accès

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) ».*

En outre, l'article 32 du RGPD stipule que *« le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».* Pareilles mesures doivent être mises en œuvre afin d'éviter notamment des accès non-autorisés aux données ou des fuites de données.

Parmi ces mesures de sécurité, la Commission nationale estime important que seules les personnes qui en ont besoin dans l'exercice de leurs fonctions et de leurs tâches professionnelles soient habilitées à avoir accès aux données nécessaires. Dans ce contexte, il est vivement recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début la personne ou le service, au sein de chaque administration concernée, qui aurait accès à l'interface informatique mise à disposition par le CTIE, et à quelles données précises cette personne ou ce service aurait accès.

En outre, il est nécessaire de prévoir un système de journalisation des accès. Enfin, la CNPD recommande que les données de journalisation soient conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.

7. Sur les échanges de données

En ce qui concerne le paragraphe (5) de l'article 13 du projet de loi, la Commission nationale tient tout d'abord à préciser que les données à caractère personnel peuvent circuler librement depuis le Grand-Duché de Luxembourg au sein de l'Espace économique européen, tant que les principes généraux du RGPD sont respectés. Il faudra notamment veiller à respecter le principe de la limitation des finalités, en vertu duquel les données ne doivent pas être traitées pour des finalités « incompatibles » avec les finalités d'origine.

Concernant le transfert de données hors de l'espace économique européen, il convient de rappeler qu'outre le respect des principes généraux du RGPD, de tels transferts devront s'opérer dans le respect des dispositions

du chapitre V du RGPD concernant les transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales.

8. Sur le droit des personnes concernées

Il convient encore de préciser que le responsable du traitement du fichier visé à l'article 13 du projet de loi, à savoir le ministre, devra respecter, lors de la collecte des données à caractère personnel auprès des personnes concernées, les dispositions de l'article 13 du RGPD, s'il les collecte directement auprès d'elles (comme cela pourrait être le cas auprès de l'acquéreur d'une arme à feu), ou les dispositions de l'article 14 du RGPD, s'il les collecte de manière indirecte (comme cela pourrait être le cas dans l'hypothèse où les fournisseurs d'armes à feu transmettraient au ministère les noms et adresses des acquéreurs). Le ministre devra fournir, selon les différentes hypothèses, toutes les informations prévues aux articles 13 ou 14 du RGPD, étant précisé qu'en cas de collecte indirecte il devra les fournir endéans les délais prévus à l'article 14, paragraphe (3) du RGPD.

9. Sur la durée de conservation des données à caractère personnel

Selon l'article 5 paragraphe (1), lettre e) du RGPD, les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées.

Au vu de ce qui précède, la CNPD se félicite qu'une durée maximale de 30 ans concernant la conservation des données ait été précisée dans le projet de loi et comprend que cette durée est nécessaire afin de permettre un traçage des armes à feu et de leurs parties essentielles aux fins de procédures administratives et pénales[158]. Cette limitation apparaît donc nécessaire et proportionnée au vu des finalités précitées.

Toutefois, concernant les autres finalités pour lesquelles les données pourraient être traitées, comme par exemple à des fins de gestion administrative, la Commission regrette que les auteurs du projet de loi n'aient pas indiqué les durées de conservation de telles données, de sorte que la CNPD n'est pas en mesure d'apprécier si en l'occurrence, le principe de durée de conservation limitée des données a été respecté concernant la collecte de ces données.

III. Sur les agréments d'armurier et de commerçant d'armes ainsi que sur les agréments des salariés et collaborateurs des armuriers

Les articles 15 (Les agréments d'armurier et de commerçant d'armes) et 17 (Salariés et collaborateurs des armuriers) du projet de loi visent à soumettre les armuriers ainsi que leurs salariés, collaborateurs, et les commerçants d'armes à un agrément du ministre afin d'exercer leur activité d'armurier ou professionnelle.

[158] Le considérant 9 de la directive dispose que : *« Compte tenu du caractère dangereux et de la durabilité des armes à feu et de leurs parties essentielles, afin de garantir que les autorités compétentes sont en mesure de tracer les armes à feu et les parties essentielles aux fins de procédure administratives et pénales et en tenant compte du droit procédural national, il est nécessaire que les enregistrements dans les fichiers de données soient conservés pendant une durée de trente ans après la destruction des armes à feu ou des parties essentielles concernées. ».*

Il convient de relever que les auteurs du projet de loi précisent au paragraphe (2) de l'article 15 que « *l'agrément ne peut être accordé qu'aux personnes physiques qui présentent les garanties d'honorabilité nécessaires (…). L'honorabilité s'apprécie sur base du comportement et des antécédents du requérant et de tous les éléments fournis par l'enquête administrative, effectuée par le Ministre suite à l'introduction d'une demande aux fins de l'octroi d'agrément* ». L'article 17 du projet de loi se réfère également à la notion d'honorabilité en ce qu'il dispose que « *L'agrément ne peut être accordé qu'aux personnes : (…) qui présentent les garanties d'honorabilité nécessaires* ».

Or, la CNPD se demande quels sont les critères d'appréciation d'une telle « *honorabilité* » alors qu'aucune précision supplémentaire n'est indiquée dans le projet de loi. De même qu'elle se demande quelles sont les vérifications susceptibles d'être opérées par le ministre dans le cadre de « *l'enquête administrative* », notamment quelles sont les données que celui-ci pourra consulter ? En effet, une telle procédure n'est pas détaillée dans le projet de la loi sous avis.

Concernant les notions d'« *honorabilité* » et d' « *enquête administrative* », il convient d'attirer l'attention des auteurs du projet de loi sur le fait que des notions similaires sont indiquées dans la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales (ci-après la « loi modifiée du 2 septembre 2011 »), le règlement grand-ducal du 1er décembre 2011 déterminant les modalités de l'instruction administrative prévue à l'article 28 de la loi modifiée du 2 septembre 2011 (ci-après le « règlement grand-ducal du 1er décembre 2011) et le règlement grand-ducal du 28 avril 2015 portant création des traitements de données à caractère personnel nécessaires à l'exécution de l'article 32 de la loi modifiée du 2 septembre 2011 (ci-après le « règlement grand-ducal du 28 avril 2015 »).

Par exemple, le chapitre 3 de la loi modifiée du 2 septembre 2011 intitulé « *L'honorabilité professionnelle* » définit cette notion et en précise les critères d'appréciation. L'article 2, paragraphe (4) du règlement grand-ducal du 1er décembre 2011 précise quant à lui les pièces devant être fournies par le demandeur et sur lesquelles son honorabilité sera appréciée.

Il convient encore de relever que l'article 28 de ladite loi dispose que : « *L'autorisation d'établissement est délivrée par le ministre après une instruction administrative. Les modalités de l'instruction administrative et les pièces à produire seront déterminées par règlement grand-ducal* ». Le paragraphe (2) de l'article 32 de la loi précitée ainsi que l'article 2 du règlement grand-ducal du 28 avril 2015 énumèrent les traitements de données à caractère personnel auxquels peut accéder le ministre dans le cadre de cette instruction administrative.

La CNPD estime, dès lors, nécessaire que les critères d'appréciation de l'honorabilité telle que visée aux articles 15 et 17 du projet de loi soient précisés, de même qu'il est également nécessaire de détailler les données auxquelles

peut accéder le ministre dans le cadre de l'enquête administrative. Les auteurs du projet de loi pourraient s'ils le souhaitent s'inspirer des dispositions légales précitées concernant la délivrance d'une autorisation d'établissement.

IV. Sur le traitement de données relatives aux infractions pénales et à la santé

Il ressort du projet de loi que les données à caractère personnel relatives à la santé (article 14 du projet de loi) et aux infractions pénales sont collectées (paragraphe (4) de l'article 13 et paragraphe (2) de l'article 22 du projet de loi) par le ministre. La Commission nationale se félicite que des bases légales aient été introduites pour le traitement des données précitées mais déplore toutefois que leurs finalités n'aient pas été précisées dans le projet de loi alors que ces traitements impliquent notamment la collecte de données sensibles au sens de l'article 9 du RGPD[159].

1. Sur le traitement des données relatives aux infractions

Tout d'abord, la Commission nationale suggère que le paragraphe (4) de l'article 13 du projet de loi concernant le traitement des données relatives au bulletin n°2 du casier judiciaire se réfère aux dispositions de l'article 8, point 1) de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire, telle qu'elle a été modifiée par une loi du 23 juillet 2016[160], comme précisé par les auteurs du projet de loi dans leur commentaire dudit article.

Il convient encore de préciser que l'article 1er du règlement grand-ducal du 23 juillet 2016 fixant la liste des administrations et personnes morales de droit public pouvant demander un bulletin N° 2 ou N° 3 du casier judiciaire avec l'accord écrit ou électronique de la personne concernée, dispose que le bulletin n°2 : *« peut être délivré sur demande et avec l'accord exprès de façon écrite ou électronique de la personne concernée »*. La Commission nationale recommande donc que le paragraphe (4) de l'article 13 se réfère à ces dispositions légales, plus particulièrement en ce qui concerne le consentement de la personne concernée.

De plus, conformément à la définition du consentement au sens du RGPD, le consentement doit être spécifique, c'est-à-dire qu'il doit correspondre à un seul traitement, pour une finalité déterminée. Dans ses lignes directrices sur le consentement au sens du RGPD, le Groupe de travail « Article 29 » précise que : *« conformément à l'article 5, paragraphe (1), point b), du RGPD, l'obtention d'un consentement valable est toujours précédée de la détermination d'une finalité déterminée, explicite et légitime pour l'activité de traitement envisagée. Combinée à la notion délimitation de la finalité de l'article 5, paragraphe (1), point b), la nécessité d'obtenir un consentement spécifique sert de garantie contre l'élargissement ou l'estompement progressif des fins auxquelles les données sont traitées après qu'une personne concernée a donné son consentement à la collecte initiale de ses données »*[161]. Or, la formulation actuelle du paragraphe (4) de l'article 13 du projet de loi en ce qu'il dispose que *« la personne concernée consent au traitement de ses données personnelles, y compris à ce que le bulletin n°2 du casier judiciaire soit délivré directement par le procureur général d'État au Ministre. »* ne permet pas de satisfaire à cette condition.

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

[160] L'article 8, paragraphe (1) de la loi du dispose que : *« Le bulletin N° 2 d'une personne physique ou morale est délivré sur demande:*
1) aux administrations de l'État, administrations communales et personnes morales de droit public saisies, dans le cadre de leurs missions légales, d'une demande présentée par la personne physique ou morale concernée, laquelle a donné son accord de manière écrite ou électronique afin que le bulletin N° 2 soit délivré directement à l'administration ou à la personne morale de droit public.
La liste des administrations et personnes morales de droit public et les motifs d'une demande de délivrance sont fixés par règlement grand-ducal; »

[161] Page 13 des lignes directrices sur le consentement au sens du RGPD, Groupe de travail « Article 29 », adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2018.

Dans un souci de clarté et compte tenu des développements qui précèdent, la Commission recommande que soit reformulé le paragraphe (4) de l'article 13 afin de refléter l'intention du législateur qui est de permettre au ministre, lorsque la personne concernée marque son accord, de demander directement auprès du procureur général d'État un bulletin n°2 du casier judiciaire. Au cas où la personne concernée ne donne pas son accord, il faudrait qu'elle fournisse elle-même le bulletin du casier. Le passage *« la personne concernée consent au traitement de ses données à caractère personnel »* devrait donc être supprimé.

La Commission nationale relève encore que les auteurs du projet de loi ont introduit de nouvelles dispositions visant à permettre, dans le cadre de la délivrance d'obtention de permis d'armes, au ministre de consulter les informations figurant au *« registre spécial prévu par l'article 15 de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse »*[162] dans l'hypothèse où le requérant serait âgé de moins de 21 ans au moment de l'introduction de la demande. Ces nouvelles dispositions prévues par la 2ième phrase du paragraphe (2) de l'article 22 du projet de loi, soulèvent certaines interrogations de la part de la Commission nationale.

En effet, les auteurs du projet de loi indiquent eux-mêmes dans leurs commentaires que ces nouvelles dispositions ont été ajoutées afin de permettre au ministre d'obtenir plus facilement l'obtention de ces informations car *« la pratique a montré qu'il y a beaucoup de réticences à fournir les informations en question au Service des armes prohibées, principalement pour des raisons, légitimes bien sûr, tenant à la confidentialité des informations concernées. ».*

Selon le principe de minimisation des données, seules les données à caractère personnel nécessaires à la réalisation des finalités doivent être traitées, compte tenu du risque que le traitement fait peser pour la vie privée des personnes concernées.

Compte tenu des développements précédents, la CNPD se demande ainsi s'il n'existerait pas des moyens alternatifs, moins intrusifs et moins attentatoires à la vie privée des mineurs concernés, mais permettant d'arriver aux mêmes finalités. Dans l'hypothèse où des moyens alternatifs ne pourraient être mis en œuvre, la Commission nationale recommande que des garanties soient prévues afin de limiter les risques d'atteintes à la vie privée des mineurs concernés. De telles garanties pourraient être mises en place en prévoyant un accès restrictif à ces données[163].

2. <u>Sur le traitement des données relatives à la santé</u>

La CNPD relève que les données relatives à l'attestation médicale sont des données sensibles au sens de l'article 9 du RGPD car elles concernent la santé des personnes concernées et rappelle que de tels traitements requièrent une protection spécifique[164] et sont soumis à des exigences plus strictes.

[162] L'article 15 de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse dispose que : « Les décisions du tribunal ou du juge de la jeunesse ne sont pas inscrites au casier judiciaire. A l'exception de celles prises en vertu de l'article 302 du code civil, elles sont toutefois mentionnées sur un registre spécial tenu par le préposé au casier judiciaire.
Sont également mentionnées sur le registre spécial les condamnations prononcées par une juridiction répressive à charge d'un mineur.
Ces décisions et condamnations peuvent être portées à la connaissance des autorités judiciaires. Elles peuvent également être portées à la connaissance des autorités administratives dans les cas où ces renseignements sont indispensables pour l'application d'une disposition légale ou réglementaire, ainsi que des tiers lésés, s'ils le demandent. »

[163] Voir point II.5) du présent avis.

[164] Voir les affaires rendues par la CJUE du 8 avril 1992, C-62/90, point 23 et du 5 octobre 1994, C-404/92 P, point 17.

De plus, il convient de soulever que le CEPD a précisé dans son avis du 17 février 2014 que : « *les « examens médicaux » devraient être définis. Les données pouvant être/susceptibles d'être traitées à ces fins devraient être énumérées de façon stricte, et des procédures de contrôle devraient être spécifiées de manière claire. Les raisons médicales de refus d'un permis devraient être indiquées clairement.* »[165].

Par ailleurs, la Commission se demande s'il ne faudrait pas préciser les critères sur lesquels doit porter l'examen médical afin de déterminer si l'état de la personne constitue ou ne constitue pas un risque pour son intégrité physique, celle d'autrui ou pour l'ordre et la sécurité publics ?

3. Remarques finales

Enfin et tel que cela a été relevé à juste titre par la Chambre de Commerce dans son avis du 2 mai 2019 sur le présent projet de loi[166], l'article 5 paragraphe (2) de la directive[167] qui prévoit un système de suivi des autorisations d'acquisition et de détention d'armes n'a pas été transposé par les auteurs du projet de loi. Il conviendrait donc de compléter l'article 22 du projet de loi afin de prévoir un tel système de suivi. Ledit système permettrait, en outre, au responsable du traitement de mettre à jour, rectifier ou supprimer les données qu'il collecte.

V. Sur le registre des armes tenu par les armuriers

La Commission nationale relève que la tenue d'un tel registre est prévu par l'article 12 de la loi modifiée du 15 mars 1983 sur les armes et munitions. L'article 19 du projet de loi concernant le registre d'armes reprend ce principe et transpose les dispositions de l'article 4, paragraphe (4), alinéa 5, de la directive.

Par ailleurs, en plus de la transposition des dispositions précitées, le paragraphe (4) de l'article 19 du projet de loi prévoit une *« connexion électronique »* par les armuriers au fichier visé à l'article 13 du projet de loi, ce qui n'est pas prévu sous l'empire de la loi du 15 mars 1983.

La CNPD se demande si ces dispositions ont pour but d'assurer un partage efficace des informations entre les armuriers et le ministre afin d'assurer un bon fonctionnement des fichiers de données, comme cela est précisé dans le considérant 10 de la directive. Dans le cadre d'un tel partage, ledit considérant prévoit notamment que *« (…) les autorités nationales compétentes devraient mettre au point un moyen de connexion électronique accessible aux armuriers et aux courtiers, qui peut inclure la transmission des informations par courrier électronique ou l'inscription directe sur une base de données ou sur un autre registre ».*

Toutefois, la Commission nationale estime que le paragraphe (4) de l'article 19 du projet de loi n'est pas rédigé avec suffisamment de précision et de clarté pour comprendre quelle est la relation que souhaitent mettre en place les auteurs du projet de loi entre les fichiers de l'article 13 et de l'article 19.

[165] Point 29, page 9 de l'Avis du CEPD.
[166] Avis de la Chambre de Commerce du 2 mai 2019 (document n°7425/01), voir ses commentaires concernant l'article 22.
[167] L'article 5 paragraphe (2) de la directive dispose que *« Les États-membres disposent de suivi, qui fonctionne de manière continue ou périodique, visant à garantir que les conditions d'octroi d'une autorisation fixées par le droit national sont remplies pour toute la durée de l'autorisation et que, notamment, les informations médicales et psychologiques pertinentes sont évaluées. Les modalités spécifiques sont déterminées conformément au droit national. Lorsque l'une des conditions d'octroi d'une autorisation n'est plus remplie, les États-membres retirent l'autorisation correspondante. »*

La CNPD se demande si l'intention des auteurs du projet de loi est de permettre aux armuriers d'avoir accès au fichier de l'article 13 du projet de loi. Dans ce cas, il conviendrait que cet accès soit strictement encadré alors que les échanges mutuels de données entre un acteur du secteur public et du secteur privé présentent certains risques d'un point de vue de la protection de la vie privée et des données à caractère personnel. La Commission nationale souligne la nécessité de respecter le principe de minimisation des données, selon lequel tout traitement de données doit être proportionné aux finalités à atteindre, compte tenu du risque que le traitement fait peser pour la vie privée des personnes concernées. De plus, la CNPD se demande à quelles données auront accès les armuriers, quels seront leurs moyens d'accès et quelles seront les mesures de sécurité mises en place dans le cadre de ces accès ?

La Commission nationale remarque encore que l'obligation de conservation d'un tel registre par l'armurier même après la cessation de son activité, tel que cela est prévu au paragraphe (3) de l'article 19, est susceptible d'être problématique. En effet, comment cette obligation de conservation minimum de 30 ans pourra être respectée en pratique si l'armurier cesse son activité au bout de 20 ans, soit avant la période minimum précitée ?

A ce titre, la CNPD constate que l'article 4, paragraphe (4), dernier alinéa de la directive ne prévoit pas une telle obligation, mais dispose que *« Lorsqu'ils cessent leurs activités, les armuriers et les courtiers remettent ce registre aux autorités nationales responsables des fichiers de données prévus au premier alinéa »*. Dès lors et dans un souci de transposition correcte de la directive en droit national, la Commission nationale recommande de reprendre littéralement les dispositions de l'article précité à ce sujet et que les auteurs du projet de loi prévoient donc que le registre soit transmis au ministre lorsque les armuriers cessent leur activité.

VI. <u>Sur l'accès par les agents de l'Administration des douanes au fichier des armes prohibées</u>

Le paragraphe (6) de l'article 52 prévoit un accès aux agents de l'Administration des douanes et accises dans le cadre de l'exercice de leurs fonctions telles que définies aux paragraphe (1) à (4) de l'article 52 précité. La CNPD regrette que le présent projet de loi ne soit pas accompagné d'un projet de règlement grand-ducal qui viendrait préciser les catégories de données auxquelles pourraient accéder les agents de l'Administration des douanes, de sorte qu'elle n'est pas en mesure d'apprécier si le principe de minimisation des données est respecté.

Par ailleurs, il ne ressort pas clairement dudit article sur quel fichier cet accès porte, car celui-ci mentionne le fichier des armes prohibées. Comme exposé au point I) du présent projet de loi, ce fichier n'est pas défini dans le projet de loi mais est mentionné dans le texte de l'ancienne loi. Cette imprécision mériterait d'être clarifiée et le législateur devrait indiquer précisément sur quel fichier cet accès porte. En effet, cela permettrait d'éviter que les agents de l'Administration des douanes et accises aient accès à un fichier lorsqu'un tel accès n'est pas justifié dans le cadre de leurs missions légales.

Enfin, la Commission nationale se félicite que les auteurs du projet de loi aient précisé les modalités d'accès au fichier des armes prohibées, de même qu'ils aient prévu une traçabilité des accès par les agents autorisés. Concernant la traçabilité des accès, il est renvoyé au point II.5.iii, du présent avis.

Ainsi décidé à Esch-sur-Alzette en date du 8 juillet 2019.

La Commission nationale pour la protection des données

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

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

Délibération n°44/2019 du 8 août 2019

Conformément à l'article 57, paragraphe 1er, lettre (c) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

Par courrier en date du 29 juillet 2019, Monsieur le Directeur du Trésor, pour le Ministre des Finances, a invité la Commission nationale à se prononcer au sujet d'amendements gouvernementaux au projet de loi n°7218 relative à des mesures macroprudentielles portant sur les crédits immobiliers résidentiels et portant modification de :

- la loi modifiée du 5 avril 1993 relative au secteur financier ;

- la loi du 1er avril 2015 portant création d'un comité du risque systémique et modifiant la loi modifiée du 23 décembre 1998 relative au statut monétaire et à la Banque centrale du Luxembourg.

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

Selon l'exposé des motifs, les amendements gouvernementaux ont pour objectif de *« donner suite aux oppositions formelles formulées par le Conseil d'État en précisant un cadre normatif strict dans lequel la CSSF peut agir lorsqu'elle décide de l'application des mesures susmentionnées ».*

ANNEXES

5

Dans son avis du 29 mars 2018 (document parlementaire 7218/06), la Commission nationale avait déjà eu l'occasion de se prononcer au sujet du projet de loi sous examen, et s'était limitée à des remarques relatives à son article 2, en particulier concernant l'utilisation des termes *« informations agrégées »*, qu'elle recommandait de remplacer par *« données agrégées et anonymisées »* (s'il s'agit en effet de données anonymes ou rendues anonymes).

La CNPD constate que les auteurs du projet de loi n'ont pas suivi cette suggestion, alors que l'article 2 du projet de loi prévoit toujours que *« (…) la Banque centrale du Luxembourg a un droit d'accès à des informations agrégées disponibles auprès d'administrations étatiques, d'établissements publics autres que ceux placés sous la surveillance des communes et d'autres autorités étatiques compétentes pour autant que ces informations soient nécessaires à ses activités de recherche et d'analyses en relation avec la mission du comité du risque systémique »*.

Or, sans plus de précisions sur ce qu'il faut entendre par *« informations agrégées »*, elle se demande si ces termes correspondent à des données anonymisées ou à des données pseudonymisées ? La Commission nationale réitère donc sa suggestion de remplacer ces termes par *« données agrégées et anonymisées »*, afin d'ôter toute ambiguïté possible sur la nature des données qui pourraient faire l'objet d'un droit d'accès par la BCL. Dans ce cas, le RGPD n'aurait pas vocation à s'appliquer à la collecte de telles données.

La CNPD entend encore rappeler à toutes fins utiles qu'au cas où les *« informations agrégées »* devraient être qualifiées de données pseudonymisées, et donc de données à caractère personnel, le RGPD s'appliquera avec toutes les conséquences qui en découlent. Or, si tel était le cas, la disposition sous examen serait manifestement trop vague et ne respecterait dès lors pas le principe de légalité et de prévisibilité qu'exige le droit et la jurisprudence européenne. En effet, comme l'explique le considérant 41 du RGPD, une base juridique ou une mesure législative qui sert de base à un traitement de données *« devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme »*.

Pour le surplus, les modifications apportées au projet de loi sous examen n'entraînent aucun changement en matière de protection des données à caractère personnel, et n'appellent par conséquent aucun commentaire supplémentaire de la part de la CNPD.

Ainsi décidé à Esch-sur-Alzette en date du 8 août 2019.

La Commission nationale pour la protection des données

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

Avis de la Commission nationale pour la protection des données relatif au fichier central de la Police grand-ducale au regard de la législation sur la protection des données.

Délibération n°45/2019 du 13 septembre 2019

Conformément à l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n° 2016/680 du 27 avril 2016 relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[168] (ci-après désignée « la Directive »), à laquelle se réfère l'article 8 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données (ci-après désignée « loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD »), «conseille la Chambre des députés, le Gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données personnelles ».

Eu égard à la mission de conseil qui lui est attribuée, la CNPD a été sollicitée par Monsieur le Ministre de la Sécurité intérieure pour rendre un avis au sujet du fichier central de la Police grand-ducale au regard de la législation en matière de protection des données.

Si le domaine des fichiers de la Police est peu connu et suscite de réelles inquiétudes des citoyens quant au respect des libertés publiques et de la protection de leurs données personnelles, les fichiers constituent néanmoins des outils indispensables à l'exécution des missions des forces de police.

Afin de répondre au mieux à la demande d'avis qui lui a été soumise, la CNPD s'est nourri des préoccupations citoyennes, des nombreuses questions parlementaires émanant des députés et des réponses à ces interrogations par les ministres concernés. La CNPD a également sollicité les autorités de la protection des données d'autres États-membres afin que ces dernières la renseignent quant au cadre légal en matière de protection des données encadrant les fichiers policiers dans leurs pays. De surcroît, au cours de l'été 2019, la CNPD s'est réunie à plusieurs reprises avec la Police grand-ducale (ci-après désignée « la Police »), dans le but d'approfondir sa compréhension de la gestion et l'exploitation qui est faite du fichier central par cette dernière.

Le présent avis se consacre exclusivement au fichier dit « central » de la Police grand-ducale. L'avis, qui n'a pas vocation à consacrer le résultat d'une enquête au sens de l'article 8, 10° de la loi du 1er août 2018 portant

[168] *JO L 119, 4.5.2016, p. 89–131*

organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, se limite à fournir une réponse à la question posée par le Ministre de la Sécurité intérieure. L'avis se divise en trois parties. Après une partie introductive sur la composition et l'utilisation du fichier central, il adresse l'utilisation dudit fichier par la Police et l'encadrement légal dont il fait l'objet. Sur la première partie, consacrée à l'encadrement du fichier central 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, s'enchaînera une analyse de la qualité de la loi encadrant le fichier central. L'avis s'achèvera sur une conclusion comprenant des recommandations à l'attention des autorités.

Introduction

Selon les explications fournies par la Police, le fichier central existe depuis que les services de police ont commencé à rédiger des procès-verbaux et rapports afin de les transmettre aux autorités judiciaires conformément à la loi, alors qu'il fallait disposer d'un outil permettant d'assurer le suivi adéquat de ces procès-verbaux et rapports. Le fichier central est opérationnel sous forme informatisée depuis 2005.

Le responsable du traitement est la Police, représentée par son Directeur général. La saisie des données, qui correspond concrètement à une digitalisation des documents rédigés par les officiers et agents de police judiciaire de la Police, est assurée par un service dédié.

Sont centralisés au sein du fichier central les procès-verbaux et les rapports de la Police. Cette centralisation a comme finalités la prévention des infractions d'une part et la recherche et la constatation des infractions d'autre part. En d'autres termes, le fichier central est un outil de travail de la Police qui est nécessaire à l'accomplissement de ses missions telles que prévues par la loi du 18 juillet 2018 sur la Police grand-ducale, ci-après désignées « la loi Police ».

Le fichier central est scindé en deux parties, l'une dite signalétique et l'autre documentaire.

Dans la partie signalétique sont renseignées des métadonnées à savoir les noms, prénoms, les alias, la date de naissance, le lieu de naissance, le pays de naissance, la nationalité, l'adresse du domicile, le numéro de matricule et, le cas échéant, la date du décès des personnes concernées. La personne concernée peut être une personne physique ou une personne morale même s'il s'agit surtout de personnes physiques.

La partie documentaire contient les procès-verbaux et les rapports regroupés au sein de dossiers. Chaque dossier correspond à une personne concernée. Un numéro de dossier unique est attribué à chaque personne concernée. Cette même personne peut être reliée à plusieurs documents différents en fonction du nombre d'affaires dans lesquelles elle est impliquée et qui ont donné lieu à un procès-verbal ou à un rapport.

Pour avoir une idée plus précise quant à la volumétrie, la configuration et l'utilisation du fichier central, des données chiffrées que la CNPD a pu inspecter directement des systèmes de la Police peuvent être utiles :

- En date du 29 juillet 2019 le système contenait 511'499 dossiers. Sur ce total, 309'175 dossiers sont dits « archivés » (i.e. l'intégralité des documents y relatifs était archivée et une consultation de ces documents n'est donc pas possible sans procédure supplémentaire). Il reste donc 202'324 dossiers pour lesquels au moins un document n'était pas archivé. A remarquer aussi que ces dossiers ne concernent pas uniquement des personnes résidentes ou de nationalité luxembourgeoise, mais toutes les personnes au nom desquelles un procès-verbal ou rapport a été rédigé par la Police. 89% des dossiers sont constitués de moins de 5 documents, 11 % des dossiers contiennent entre 6 et 50 documents et moins de 1% des dossiers contiennent plus de 50 documents.

- Sur la période de 2010 jusqu'à 2019, en moyenne 15'157 nouveaux dossiers ont été créés par année. En termes de nouveaux documents ainsi injectés dans le système, cela revient à une moyenne de 55'947 documents/année. Il est à remarquer que ces chiffres ne varient pas significativement sur cette période.

- Sur la période de 2010 jusqu'à 2019, en moyenne 176'550 recherches ont été effectuées par année dans le système pour identifier la présence ou non d'une personne dans le système. Il est cependant à remarquer que les recherches avaient atteint un sommet en 2012 avec 239'460 recherches et sont depuis lors en déclin permanent et se situent pour l'année 2018 à 114'802. Il s'agit dès lors d'une diminution de plus de la moitié sur les 7 dernières années. A noter qu'une recherche d'un dossier ne signifie pas que le dossier a effectivement été consulté. En effet, sur la période de 2010 jusqu'à 2019, en moyenne 36'805 dossiers ont été consultés par année. Le nombre de consultations de dossiers avait atteint un sommet en 2012 avec 60'270 consultations et depuis lors, il est en déclin quasi permanent et se situe pour l'année 2018 à 21'187 consultations, à savoir une diminution d'environ 2/3 des consultations sur les 7 dernières années.

Selon les informations de la Police, l'accès au fichier central est accordé d'office à chaque nouvel agent ou officier de police judiciaire, étant donné qu'il pourra être amené à travailler avec cet outil. En ce qui concerne l'accès et l'utilisation du fichier central, il est cependant important de préciser que ce n'est pas parce qu'un policier dispose d'un accès au fichier central qu'il peut en faire usage comme il le souhaite. Ladite utilisation doit correspondre à des finalités déterminées, explicites et légitimes et ne peut être incompatible avec celles-ci. A titre d'exemple un policier n'a pas le droit de rechercher ou consulter des personnes qui ne sont pas en lien avec les dossiers qu'il est en train de traiter. Les logs qui sont générés lors de recherches et de consultations servent notamment à pouvoir détecter de tels abus.

Lors d'un contrôle de police administrative, la consultation du fichier central se limite généralement à la partie signalétique. Dans ce cas de figure, les officiers et/ou les agents de police n'ont pas accès à distance direct au fichier central via un dispositif mobile. L'accès ne peut se faire qu'à partir d'un poste de travail hébergé dans les locaux

sécurisés de la Police. Ainsi, les policiers sont tenus de contacter leurs collègues via le Réseau National Intégré de Radiocommunication (ci-après désigné « RENITA »), qui effectuent en interne la recherche sur une personne donnée. Cette requête permet aux policiers sur le terrain de vérifier si la personne concernée par l'intervention ou le contrôle fait l'objet d'un signalement ou non. Au sein de la partie signalétique du fichier central, la recherche d'une personne en entrant son nom ou une autre métadonnée la concernant est possible.

Les recherches effectuées sont loguées sous le nom du policier qui a réalisé la recherche et non pas celui qui a effectué la demande au préalable. Le retraçage des appels des policiers sur le terrain n'est pour le moment pas réalisé.

Lors de la consultation d'un dossier d'une personne concernée au sein du fichier central, un motif de recherche de la partie documentaire du fichier central doit être entré afin de s'assurer de la justification et de la légitimité de l'utilisation des données contenues dans le fichier central. Il peut s'agir de motifs libres ou des motifs prédéfinis. Les motifs prédéfinis sont au nombre de dix-huit. Il sont dénommés de la manière suivantes : « contrôle frontière extérieure (aéroport) », « contrôle aux frontières intérieures », « contrôle cadre police des étrangers », « contrôle cadre alerte de police », « contrôle flagrant délit/crime », « contrôle dans service d'ordre », « contrôle cadre contrôle national », « contrôle dans enquête judiciaire », « contrôle stupéfiants », « contrôle mœurs », « contrôle vol de véhicules », « contrôle entraide judiciaire », « contrôle code de la route », « contrôle cadre environnement », « contrôle armes prohibées », « contrôle dans enquête douanière », « contrôle SLCPI »[169]. Les trois motifs les plus utilisés sont : « contrôle cadre contrôle national », le « contrôle SLCPI » et le « contrôle dans service d'ordre ».

Pour avoir une idée plus précise quant aux accès du fichier central, des données chiffrées que la CNPD a pu inspecter directement des systèmes de la Police peuvent être utiles :

- En date du 30 juillet 2019, un total de 1840 personnes disposaient des accès logiques nécessaires afin de pouvoir utiliser le système pour effectuer des recherches respectivement consulter des dossiers. A noter qu'à cette même date, seuls 36 personnes disposaient des autorisations qui leur permettaient de créer un nouveau dossier. A rappeler que le fait de disposer des accès logiques exprime la possibilité d'utiliser le système, mais n'en dit rien sur l'utilisation effectivement faite - qui doit être motivé par un besoin concret par rapport à un dossier.

- Sur les 6 premiers mois de l'année 2019, 69 policiers ont effectués plus que 100 recherches (i.e. recherche pour identifier la présence ou l'absence d'un dossier). Une grande partie des membres de la police semblent utiliser le système de manière plus ponctuelle. En effet, sur cette période, 589 policiers ont réalisé entre 0 et 10 recherches et 487 policiers ont réalisé entre 11 et 100 recherches. Il est à noter qu'afin de pouvoir consulter un dossier, il faut tout d'abord effectuer une recherche pour l'identifier. De ce fait le nombre de consultations effectives de dossiers est de fait donc inférieur au nombre de recherches effectuées. Ainsi, que 19 policiers ont donc effectivement consulté plus que 100 dossiers sur la période indiquée.

[169] service /ou section de liaison de la coopération policière internationale.

La consultation et l'utilisation des données archivées sont beaucoup plus restreintes. En effet, l'accès aux données archivées dans le fichier central s'effectue sur demande et doit être accordée par le Procureur général d'État ou un membre de son parquet délégué. La consultation avait originairement été basée sur l'article 2 paragraphe 1er alinéa 3 du règlement grand-ducal du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale, c'est-à-dire le règlement « Ingepol » qui pour sa part n'avait jamais vraiment été mis en œuvre, mais dont certains critères avaient été appliquées au fichier central même au-delà de l'abrogation de ce règlement au moment de l'entrée en application de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données qui opère une réforme en matière de protection des données et ce également pour le volet dit police/justice. En effet, cette loi abrogeait la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Dans le cadre d'une demande d'accès aux données archivées sont notamment renseignés les éléments suivants : la date de la demande, le login du demandeur, le nom du Procureur général d'État ou un membre de son parquet délégué qui a accordé l'accès et la période pendant laquelle l'archive peut être consultée. A noter que le nombre d'accès aux archives est toutefois plus limité puisqu'au 18 juillet 2019 avaient été enregistrées 106 demandes et ce, depuis 2005.

Après cet aperçu factuel du contenu et du fonctionnement du fichier central, il y a à présent lieu d'examiner le fichier central au regard 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.

I. L'encadrement légal du fichier central par la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale

La Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (« Directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale » ou « la Directive »), a pour objet de protéger les données à caractère personnel collectées et traitées à des fins de justice pénale.

Au niveau de l'UE, la protection des données dans le secteur de la police et de la justice pénale est réglementée dans le contexte du traitement transfrontalier et national par des autorités de police et de justice pénale des États-membres et des acteurs de l'UE. Au niveau des États-membres, la directive relative à la protection des données pour les autorités policières et judiciaires en matière pénale doit être transposée en droit national.

ANNEXES

5

Dans son « Manuel de droit européen en matière de protection des données », l'Agence des droits fondamentaux de l'Union européenne précise ce qui suit : *« La directive s'appuie, dans une large mesure, sur les principes et définitions énoncés dans le Règlement général sur la protection des données (« RGPD »), en tenant compte de la nature spécifique des domaines de la police et de la justice pénale. Mais bien que ces notions s'inspirent du RGPD, la directive les traite sous l'angle spécifique des autorités policières et judiciaires en matière pénale. Par rapport au traitement des données à des fins commerciales, qui est régi par le règlement, le traitement de données liées à la sécurité peut nécessiter un certain degré de flexibilité. Ainsi, la fourniture du même niveau de protection aux personnes concernées en termes de droit à l'information, de droit d'accès à leurs données personnelles ou d'effacement de celles-ci, telle qu'elle est prévue par le RGPD, pourrait avoir pour conséquence qu'une mission de surveillance menée à des fins répressives deviendrait inefficace dans un contexte répressif. La directive ne fait donc pas référence au principe de la transparence.*

De même, les principes de minimisation des données et de limitation de la finalité, qui imposent que les données à caractère personnel soient limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées et qu'elles soient traitées pour des finalités déterminées et explicites, doivent aussi être appliqués de manière flexible au traitement de données liées à la sécurité. Les informations collectées et conservées par les autorités compétentes pour une affaire particulière peuvent se révéler extrêmement utiles pour la résolution d'affaires futures. »[170]

La Directive est transposée en droit 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 (ci-après désignée « la loi » ou « la loi de transposition »), qui prévoit de manière générale et encadre l'ingérence qui est faite par les traitements mis en œuvre par les fichiers dans les droits fondamentaux. En effet, cette loi a pour objet de transposer la directive en droit luxembourgeois et de facto, de fixer des règles minimales spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes visées à l'article 1 de cette loi. En d'autres termes, même si cette loi n'est pas spécifiquement dédiée à la gestion et l'exploitation du fichier central, elle encadre néanmoins les traitements dudit fichier utilisé par la Police dans le cadre des missions qui lui sont conférées par la loi du 18 juillet 2018 sur la Police grand-ducale.

A titre liminaire, il y a lieu d'analyser les dispositions applicables au traitement des données à caractère personnel effectué via le fichier central (A) puis de faire état des droits des personnes concernées par le traitement de leurs données à caractère personnel à travers le fichier central (B) pour enfin examiner les obligations du responsable du traitement quant à la gestion et l'exploitation dudit fichier (C).

A. Les principes applicables au traitement des données à caractère personnel effectué via le fichier central

A travers le fichier central, la Police, autorité compétente au sens de la loi de transposition[171], effectue un traitement de données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de

[170] Édition 2018, p. 315-317.
[171] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 2 paragraphe 1 point 7.

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[172].

Cette loi reprend la définition du fichier telle qu'établie par la directive[173] à savoir *« tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »*[174]. Étant donné que le fichier central est une base de données comprenant à la fois un ensemble de métadonnées et des dossiers, il correspond à la présente définition.

L'article 3 de la loi de transposition énonce les principes que le traitement de données à caractère personnel doit respecter et fixe le cadre auquel le responsable du traitement doit se conformer. Dans les articles suivants, la loi énonce quelques dispositions spécifiques applicables au traitement des données à caractère personnel. Il s'agit, entre autres, de la mise en place des délais de conservation et d'examen (1), la distinction entre les différentes catégories de personnes concernées (2), la distinction entre les données à caractère personnel et vérification de la qualité des données à caractère personnel (3), de la licéité du traitement (4) et le traitement portant sur des catégories particulières de données à caractère personnel (5).

1) Les délais de conservation et d'examen

L'article 5 de la Directive donne une marge de manœuvre aux États-membres dans la fixation des délais appropriés pour l'effacement des données à caractère personnel et la vérification de la nécessité de conserver lesdites données. Elle mentionne par ailleurs que des règles procédurales doivent garantir le respect des délais en question[175].

Dans son avis du 28 décembre 2017 relatif au projet de loi (n°7168) de transposition de la directive, la CNPD avait estimé que l'article 5 de la directive n'était pas correctement transposé en droit national. Le législateur n'a cependant pas suivi l'argumentation de la CNPD.

Ainsi, le législateur luxembourgeois a choisi de confier au responsable du traitement la fixation des délais de conservation des données ainsi que les règles procédurales en vue d'assurer le respect de ces délais[176].

En l'espèce, il revient donc au Directeur général de la Police d'établir un délai d'effacement des données à caractère personnel et de veiller à ce que la durée de conservation de ces dernières au sein du fichier central n'excède pas ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées[177].

Dans sa réponse à la question parlementaire n°752, le Ministre de la Sécurité intérieure, indique que toutes les données à caractère personnel sont conservées 10 ans à partir de leur enregistrement au sein du fichier central. Une telle durée tient compte des délais de prescription tels que prévus par le Code de procédure pénale, à savoir 5 ans

[172] *Ibidem,* article 1er paragraphe 1.
[173] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO L 119, 4.5.2016, p. 89–131*, article 3 paragraphe 6.
[174] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 2 paragraphe 1 point 6.
[175] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO L 119, 4.5.2016, p. 89–131*, article 5.
[176] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 4.
[177] *Ibidem,* considérant 26.

pour les délits[178] et 10 ans pour les crimes[179]. Selon la Police, l'application d'un même délai présente l'avantage de se retrouver avec un délai identique pour les crimes et les délits. Une distinction entre la gravité des faits basée sur la catégorie d'infraction ne s'impose plus entre le crime et le délit si le principe d'un délai initial fixe est maintenu. La distinction en fonction de la catégorie d'infraction était par ailleurs toujours délicate, alors qu'une même infraction peut répondre à plusieurs qualifications, qui peuvent relever de différentes catégories, et qui peuvent évoluer au cours de la procédure pénale. Par ailleurs, les faits, à la base d'une catégorie d'infraction constatée par la Police, sont susceptibles d'être requalifiés par la suite par les autorités judiciaires aux cours de la procédure.

D'après les informations de la Police, les données relatives aux contraventions ne seraient actuellement plus conservées dans le fichier central.

A l'expiration du délai de 10 ans, les données sont automatiquement archivées et elles sont censées être effacées 60 ans après leur premier enregistrement tel qu'il était prévu par le règlement grand-ducal de 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale[180]. A ce sujet, la CNPD est d'avis que la durée d'archivage des données est disproportionnée au regard des finalités du fichier central et des missions de la Police.

Les demandes d'accès à la partie archivage, qui doivent être motivées par rapport à l'affaire en cours dans le cadre de laquelle l'accès est demandé, sont traitées au cas par cas par le Procureur général d'État ou un de ses adjoints et l'accès est autorisé s'il résulte de la motivation de la demande, par exemple, que ces données sont nécessaires dans le cadre d'une poursuite pénale nationale ou internationale actuelle. La CNPD s'interroge quant à la pertinence de l'application dudit règlement en l'espèce et sur le caractère proportionné dudit délai. En effet, la CNPD s'est à de nombreuses reprises prononcée quant au caractère désuet du règlement grand-ducal en question et la nécessité de tenir compte de l'évolution de la législation en matière du droit à la protection des données à caractère personnel[181]. Elle estime, que le besoin de conservation devrait s'appliquer en fonction de l'issue d'une affaire tel que le classement sans suite, le non-lieu, l'acquittement, la condamnation ou la réhabilitation, tout en préservant toutes les garanties des personnes intéressées en cas de révision, ainsi que la flexibilité nécessaire pour mener à bon terme ses missions. Or, sans un retour qualifié de la part des autorités judiciaires, la Police n'est pas en mesure de répondre à ses obligations de mises à jour ou d'effacement des données.

La CNPD salue d'autant plus la réponse à la question parlementaire n°752, selon laquelle la Police et le Ministère Public travaillent à la mise en place d'un système de transmission automatisé d'informations succinctes sur le suivi réservé par les autorités judiciaires aux procès-verbaux transmis par la Police.

[178] Article 638 du Code de procédure pénale.
[179] *Ibidem,* article 637.
[180] Article 8 paragraphe 2.
[181] Voir notamment les avis suivants :
Avis complémentaire du 1er décembre 2017 de la Commission nationale pour la protection des données relatif au projet de loi n°7045 sur la Police grand-ducale et portant modification et abrogation de plusieurs dispositions légales.
Point 4 de l'avis du 24 mars 2017 de la Commission nationale pour la protection des données relatif au projet de loi n°7044 portant réforme de l'Inspection générale de la Police, du projet de règlement grand-ducal relatif au fonctionnement de l'Inspection générale de la Police et au projet de loi n°7045 portant réforme de la Police grand-ducale,
Point 1.1 de l'avis du 17 novembre 2016 de la Commission nationale pour la protection des données relatif au projet de loi n°6976 relatif à l'échange de donnée à caractère personnel et d'informations en matière policière,
Point 3 de l'avis du 30 juillet 2015 de la Commission nationale pour la protection des données relatif au projet de loi n°6759 portant approbation du « *Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information* », signé à Luxembourg le 20 juin 2012 et au projet de loi n°6762 portant approbation de l'Accord entre le Gouvernement de Luxembourg et de Gouvernement des États-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave, signé à Luxembourg le 3 février 2012,
Avis du 25 juillet 2013 de la Commission nationale pour la protection des données relatif au projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière.

Il peut également être ajouté que la police n'avait pas mis en place des règles procédurales[182] en vue d'assurer le respect des délais de conservation, ainsi que de la proportionnalité[183] de la durée de conservation des données à caractère personnel, compte tenu de l'objet du fichier et de la nature ou de la gravité des infractions et faits concernés tels que prévus par la loi de transposition.

2) La distinction entre différentes catégories de personnes concernées

LA CNPD a constaté qu'au sein des documents repris dans le système, il n'est pas techniquement possible de faire une distinction de manière structurée entre les personnes ayant commis une infraction (ou suspectée d'avoir commis une infraction), les personnes reconnues coupables d'une infraction pénale, des victimes d'infractions pénales, les tiers à une infraction pénale telles que les témoins, des contacts ou des associés aux personnes précédemment visées tel que prévu à la fois par la Directive[184] et par la loi de transposition[185]. Les dossiers et les documents qui sont contenus dans le fichier ne sont donc pas classés en fonction de la qualité de la personne concernée.

3) La distinction entre les données à caractère personnel et vérification de la qualité des données à caractère personnel

La Directive dispose que les États-membres prévoient que les données à caractère personnel fondées sur des faits sont, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles[186].

Elle dispose également que toutes les données à caractère personnel qui ne sont pas à jour ne peuvent être transmises ou mises à disposition[187]. En transposant la Directive, la loi de transposition reprend de telles dispositions.

Au cours des travaux qu'elle a menés, la CNPD n'a pas constaté l'existence d'appréciations personnelles au sein du fichier central. La CNPD n'a toutefois pas non plus pu constater la mise en œuvre d'une procédure de vérification quant à la qualité des données à caractère personnel par la Police. A cet égard, il peut être mentionné que la quasi absence de retours des autorités judiciaires à l'égard de la Police en ce qui concerne les dossiers qui lui sont transférés apparaît compromettre l'existence d'une telle vérification. Un système de transmission automatisé d'informations sur le suivi des affaires effectué par les autorités judiciaires devrait néanmoins voir le jour et favoriser la mise à jour des données contenues au sein du fichier central[188].

[182] Art 4 (2) 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.
[183] Art 7 (2) 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.
[184] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO L 119, 4.5.2016, p. 89–131*, article 6.
[185] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 5.
[186] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO L 119, 4.5.2016, p. 89–131*, article 7 paragraphe 1.
[187] *Ibidem,* article 7 paragraphe 2.
[188] La réponse à la question parlementaire n°752 « La Police et le Ministère Public travaillent à la mise en place d'un système de transmission automatisé d'informations succinctes sur le suivi réservé par les autorités judiciaires aux procès-verbaux transmis par la Police afin notamment d'assurer qu'en cas d'acquittement, l'accès aux données par les policiers soit supprimé et que les données en question soient transférées à la partie archivage où elles ne peuvent être accédées que sur autorisation écrite du Procureur général d'État ou d'un de ses adjoints ».

4) Les finalités

Dans le cadre de la Directive, les responsables de traitement sont des autorités publiques compétentes ou d'autres organismes investis de prérogatives de puissance publique, qui déterminent les finalités et les moyens du traitement de données à caractère personnel. La directive impose plusieurs obligations au responsable du traitement afin d'assurer un niveau élevé de protection des données à caractère personnel traitées à des fins répressives[189].

Tandis que la Directive dispose que les États-membres doivent prévoir que le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour des finalités énoncées à l'article 1er, paragraphe 1er[190] , et où il est fondé sur le droit de l'Union ou le droit d'un État-membre, la loi de transposition prévoit que ce même traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution des missions de l'autorité compétente […] pour une des finalités énoncées à l'article 1er et lorsque cette mission est effectuée en application des dispositions législatives régissant l'autorité compétente visée. Cette transposition réduit le champ des hypothèses dans lesquelles un traitement peut être licite à celles, où les missions à l'exécution desquelles il est nécessaire sont effectuées en application des dispositions législatives régissant l'autorité compétente visée, en l'espèce la Police et dont les finalités sont couvertes par l'article 1er de la Directive. Il s'ensuit, que même en l'absence d'une législation ou d'une documentation plus explicite sur les finalités spécifiques du fichier central, sa licéité ne peut pas être contestée.

5) Le traitement portant sur des catégories particulières de données à caractère personnel au sein du fichier central

Les données sensibles doivent faire l'objet d'une protection particulière lorsqu'elles font l'objet de traitements et ceux-ci ne doivent intervenir que dans des cas de nécessité absolue et se limiter aux conditions suivantes :

« a) lorsqu'ils sont autorisés par le droit de l'Union européenne ou en application de la présente loi ou d'une autre disposition du droit luxembourgeois ;
b) pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique, ou
c) lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée »[191].

Au cours des travaux effectués, la CNPD n'a pas pu constater la mise en œuvre de mesures offrant des garanties supplémentaires spécifiques quant aux traitements de données sensibles effectués par la Police à travers le fichier central.

Le traitement mis en œuvre par la Police à travers ledit fichier doit également conférer un degré de protection particulier à l'égard des personnes physiques mineures et ce, conformément au considérant 50 de la Directive 2016/680[192], qui dans son corps de texte ne prévoit pas de garanties particulières pour les mineurs et a fortiori, sa

[189] Manuel de droit européen en matière de protection des données, Édition 2018, Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, p. 320.
[190] Article premier, 1. La présente directive établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénale, 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.
[191] *Ibidem,* article 9.
[192] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO L 119, 4.5.2016, p. 89–131*, considérant 50.

loi de transposition non plus. Par contre, la loi du 10 août 1992 relative à la protection de la jeunesse souligne le besoin d'une telle protection à part entière même si celle-ci ne prévoit pas explicitement la protection des données des personnes physiques mineures en tant que telle[193]. Ainsi, le statut particulier des mineurs et les règles de la loi de 1992 requièrent le respect de critères de traitement particuliers, se traduisant au niveau de l'enregistrement, de la conservation, de l'accès et de l'utilisation ultérieure de ces données.

Pour avoir une idée plus précise quant aux accès du fichier central, des données chiffrées que la CNPD a pu inspecter directement des systèmes de la Police peuvent être utiles :

- Sur la période de 2010 jusqu'à 2019, en moyenne 849 nouveaux dossiers ont été créés par année qui concernent des mineurs. Il est à remarquer que ces créations avaient atteint un sommet en 2013 avec 1'239 nouveaux dossiers et par la suite ont diminué en 2018 à 638 nouveaux dossiers.

- Sur la période de 2010 jusqu'à 2019, en moyenne 820 dossiers ont été consultés par année. Il est à noter qu'afin de pouvoir consulter un dossier il faut tout d'abord effectuer une recherche pour l'identifier. Les consultations des dossiers avaient atteint un sommet en 2013 avec 1'622 consultations et par la suite ont diminué en 2018 à 423 consultations.

Malgré une présence claire de documents concernant des mineurs au sein du fichier central, une mise en œuvre de garanties spécifiques relatives aux traitements des données à caractère personnel de ces derniers fait défaut. Sur question, il nous a été confirmé qu'un champ texte libre au sein du dossier serait utilisé pour rendre les policiers attentifs au fait qu'il s'agit d'un mineur.

B. Les droits des personnes concernées par le traitement de leurs données à caractère personnel à travers le fichier central

La directive confère à l'égard des personnes concernées des droits relatifs aux traitements de leurs données à caractère personnel afin de permettre à ces dernières de garder le contrôle sur celles-ci. Il revient au responsable du traitement de faciliter l'exercice de ces droits et il se doit de fournir des informations concises, compréhensibles et aisément accessibles en des termes clairs et simples et ce, via des moyens appropriés.

La loi de transposition de la Directive reprend lesdits droits, bien qu'avec une certaine flexibilité et un moindre degré de transparence comparé aux droits de la personne concernée tels qu'ils découlent du RGPD. Les personnes dont les données à caractère personnel font l'objet d'un traitement doivent être informées par le responsable du traitement quant audit traitement (1), les personnes concernées peuvent également exercer un droit d'accès à leurs données (2) et elles disposent d'un droit de rectification ou d'effacement des données (3). Or, selon le cas, la Police peut retarder ou limiter, en tout ou en partie, l'exercice des droits des personnes concernées (4).

[193] La qualité de la loi du 10 août 1992 relative à la protection de la jeunesse à cet égard fait l'objet de discussions au sein de la Partie II du présent avis.

1) L'information des personnes concernées par le responsable du traitement

La Directive[194] et la loi de transposition déterminent un minimum de données que le responsable du traitement doit mettre à la disposition de la personne concernée[195]. Il incombe à la Police de fournir aux personnes dont les données sont traitées au sein du fichier central l'identité et les coordonnées du responsable du traitement, les coordonnées du délégué à la protection des données, les finalités du traitement auquel sont destinées les données à caractère personnel, la possibilité d'introduire une réclamation auprès de la CNPD ou l'Autorité de contrôle judiciaire et la faculté d'exercer le droit d'accès aux données à caractère personnel, leur rectification ou leur effacement.

Le responsable du traitement peut, dans des cas particuliers, fournir des informations complémentaires afin de permettre à la personne concernée de faire valoir ses droits. Il s'agit de la base juridique du traitement, la durée de conservation des données à caractère personnel ou les critères utilisés pour déterminer ladite durée. Le responsable du traitement peut également indiquer les catégories de destinataires des données en question et dire si celles-ci ont été collectées à l'insu de la personne concernée ou non[196].

La CNPD a pu constater que la Police publie un nombre d'informations générales sur son site internet dont son adresse, les coordonnées du délégué à la protection des données et les droits conférés aux personnes concernées[197]. Une information plus spécifique quant au traitement de données à travers le fichier central fait défaut.

2) Droit d'accès de la personne concernée

Conformément à la Directive[198] et à la loi de transposition[199], les personnes concernées peuvent demander à la Police si leurs données à caractère personnel sont contenues ou non au sein du fichier central et si par conséquent elles font l'objet d'un traitement par la Police. Lors d'une réponse affirmative à une telle interrogation, l'accès aux données peut être obtenu concernant les informations relatives aux finalités du traitement ainsi que de sa base juridique, aux catégories de données à caractère personnel concernées, aux destinataires qui sont établis dans des pays tiers ou les organisations internationales. La Police, lorsque cela est possible, est également tenue d'indiquer la durée de conservation des données à caractère personnel ou les critères appliqués pour déterminer la durée de la conservation. Dans un tel cas de figure, la Police doit également informer la personne concernée de son droit de rectification ou d'effacement. Le droit d'introduire une réclamation auprès de la CNPD et de l'Autorité de contrôle judiciaire doit également être communiqué, tout comme les données faisant l'objet d'un traitement en cours et des informations relatives à leurs sources.

[194] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO L 119, 4.5.2016*, p. 89–131, article 13.

[195] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 12, paragraphe 1.

[196] *Ibidem*, article 12, paragraphe 2.

[197] Voir les publications sur le site internet de la Police grand-ducale à la page https://police.public.lu/fr/support/aspects-legaux/2018-rgpd.html, consultée pour la dernière fois le 29/08/ 2019.

[198] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO L 119, 4.5.2016, p. 89–131*, article 14.

[199] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 13.

La Police a prévu des procédures pour la mise en œuvre du droit d'accès des personnes qui en font la demande. La possibilité d'effectuer ledit droit, les démarches à réaliser ainsi que les coordonnées du délégué à la protection des données de la Police sont affichées publiquement sur son site internet[200].

3) Droit de rectification ou d'effacement des données à caractère personnel

Il incombe au responsable du traitement de rectifier les données qui sont inexactes. Les données doivent être effacées par le responsable du traitement lorsque le traitement de ces données constitue une violation des principes énoncés par la loi de transposition, une violation de la licéité du traitement ou encore une violation des dispositions relatives aux données sensibles. L'effacement peut également intervenir lorsque le responsable du traitement y est contraint afin de respecter une obligation légale[201].

Les destinataires des données à caractère personnel doivent être informés de l'effacement ou de la rectification des données par le responsable du traitement afin d'en tenir compte[202].

Fait est de constater que la Police communique quant à la possibilité qu'ont les personnes concernées d'exercer leur droit de rectification ou d'effacement des données à caractère personnel[203].

4) La limitation des droits reconnus aux personnes concernées

En raison de la nature spécifique des activités policières, la Directive et a fortiori la loi de transposition, prévoient que la Police peut limiter les droits des personnes concernées. La Police peut ainsi retarder, limiter ou refuser l'information des personnes concernées ou encore leur limiter complètement ou partiellement l'accès aux données les concernant[204]. Cette limitation doit être nécessaire et proportionnée dans une société démocratique en tenant compte de la finalité du traitement en question et tenir compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée. Par conséquent, la Police doit apprécier au cas par cas si elle invoque une limitation, afin :

- d'éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires,
- d'éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales,
- de protéger la sécurité publique,
- de protéger la sécurité nationale et la défense nationale, ou
- de protéger les droits et les libertés d'autrui.

[200] Voir les publications sur le site internet de la Police grand-ducale à la page https://police.public.lu/fr/support/aspects-legaux/2018-rgpd.html, consultée pour la dernière fois le 29/08/ 2019.
[201] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 15 paragraphe 2.
[202] *Ibidem*, article 15 paragraphe 6.
[203] https://police.public.lu/fr/support/aspects-legaux/2018-rgpd.html, consultée pour la dernière fois le 29/08/ 2019.
[204] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 12 paragraphe 3, article 14, article 15 paragraphe 4.

Lorsque la Police oppose à une personne concernée une limitation de ses droits, elle est toutefois tenue d'informer la personne concernée de la possibilité qu'elle a d'exercer ses droits par l'intermédiaire de la CNPD ou de l'Autorité de contrôle judiciaire. Au cas où la personne concernée fait usage de cette possibilité, la CNPD ou l'Autorité de contrôle judiciaire informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. L'autorité de contrôle compétente informe également la personne concernée de son droit de former un recours juridictionnel.[205]

La CNPD ne dispose pas d'informations quant à la limitation des droits des individus mis en œuvre par la Police et ne peut donc pas se prononcer quant à la proportionnalité des procédures appliquées.

Après avoir analysé les droits à la disposition des personnes concernées pour contrôler leurs données à caractère personnel alors que celles-ci font l'objet d'un traitement par la Police via le fichier central, il y a lieu à présent de revenir sur les obligations que doit remplir le responsable du traitement.

C. Les obligations du responsable du traitement quant à la gestion et l'exploitation dudit fichier

L'entrée en application du RGPD et de la Directive occasionne un changement de paradigme puisqu'elle vise à responsabiliser les responsables de traitement dans la vérification et le contrôle de la légalité des traitements des données à caractère personnel qu'ils mettent en œuvre ainsi que la mise en place de garanties adéquates afin de protéger les personnes concernées par lesdits traitements. Le système de l'autorisation préalable que ce soit par demande auprès de la CNPD ou par règlement grand-ducal et de la notification préalable pour traiter les données à caractère personnel n'est donc plus de mise. Le régime du contrôle a priori laisse à présent place à un système de contrôle a posteriori par l'autorité de contrôle afin d'apprécier la conformité du traitement avec le cadre légal en matière de protection des données applicable à différents égards, à savoir, le respect des principes énoncés par la Directive, voire sa loi de transposition, le respect des droits de la personne concernée, ainsi que des obligations du responsable du traitement.

La Directive et la loi de transposition définissent ce qu'est un responsable du traitement. Ainsi, le responsable du traitement est *« l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union européenne ou le droit luxembourgeois, le responsable du traitement ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union européenne ou le droit luxembourgeois »*[206]. En l'espèce, l'autorité compétente qui détermine les finalités et les moyens du traitement est la Police grand-ducale représentée par son Directeur général.

La Directive[207] et la loi[208] de transposition confèrent des obligations au responsable du traitement. La Police se doit de prendre des mesures appropriées et effectives pour garantir et pouvoir démontrer à tout moment que le

[205] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 16.
[206] *Ibidem*, article 2 paragraphe 8.
[207] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, article 19 et suivants.
[208] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 18 et suivants.

traitement des données à caractère personnel est effectué de manière à préserver les droits et libertés des personnes concernées dans une société démocratique. Il incombe à la Police de respecter le juste équilibre entre l'exercice de ses missions et l'observation de politiques appropriées en matière de protection des données.

Il s'agit d'obligations générales 1), d'une obligation quant à la sécurité des données 2) et une obligation quant à la désignation d'un délégué à la protection des données 3).

1) Les obligations générales

Les obligations générales qui incombent à la Police en ce qui concerne la gestion et l'exploitation du fichier central sont : la protection des données dès la conception et la protection des données par défaut a), la tenue d'un registre d'activités de traitement b), la journalisation c) et l'analyse d'impact d).

a) La protection des données dès la conception et la protection des données par défaut

Il incombe au responsable de traitement lors de la gestion et de l'exploitation d'un fichier comme le fichier central, d'intégrer, dès la conception du fichier ou une fois que celui-ci est opérationnel, le respect et la mise en œuvre des principes relatifs à la protection des données.

Ainsi, par défaut, la Police doit notamment s'assurer que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique au traitement sont traitées et que leur accès soit limité au minimum.

La protection des données dès la conception et par défaut sont des obligations introduites par le RGPD et la Directive. Tandis que la CNPD reconnait que de *facto,* elles n'existaient donc pas lorsque le fichier central fut créé, la CNPD estime néanmoins que la réévaluation permanente de l'adéquation des mesures de protection de données implémentées quant aux obligations légales qui lui incombent, aurait dû amener la Police à une revue approfondie, voire même une refonte des mécanismes d'accès au niveau du fichier central.

En effet, un accès permanent au fichier central pour quasiment 2'000 policiers, même en absence de cas d'abus démontré, comparé à la réelle nécessité de consultation sur le terrain, doit être considérée comme inadéquat. Même en l'absence d'une refonte approfondie du mécanisme d'accès, la CNPD estime que la Police aurait pu et dû implémenter des mesures comme la mise en place de revues de logs pour détecter d'éventuels accès douteux pour mitiger le risque d'abus et assurer la protection des données des citoyens.

b) Registre des activités de traitement

Pour pouvoir apporter la preuve qu'il respecte les obligations lui imposé par la Directive, respectivement la loi de

transposition, le responsable du traitement doit documenter en interne ses activités de traitement de données. Ainsi, la loi de transposition impose au responsable du traitement de tenir un registre de toutes les catégories d'activités de traitement effectuées sous sa responsabilité. Elle prévoit d'une manière claire et précise les informations qui doivent y figurer, à savoir :

« a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement et du délégué à la protection des données ;
b) les finalités du traitement ;
c) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
d) une description des catégories de personnes concernées et des catégories de données à caractère personnel,
e) le cas échéant, le recours au profilage ;
f) le cas échéant les catégories de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ;
g) une indication de la base juridique de l'opération de traitement, y compris les transferts, à laquelle les données à caractère personnel sont destinées ;
h) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données à caractère personnel ;
i) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 28, paragraphe 1[209] *»*[210].

Le 5 juillet 2019 et conformément à la loi de transposition[211], la Police a mis son registre de traitement à disposition de la CNPD. La CNPD a constaté que le registre contient des informations relatives au fichier central, mais que celles-ci sont incomplètes. La CNPD attire l'attention sur le rôle primordial qui revient à ce registre quant à la conformité des traitements avec la loi. En effet, la Police n'est pas en mesure de se conformer au principe de responsabilisation tant qu'elle n'a pas inventorié l'intégralité des traitements avec un niveau de détail minimal tel qu'exigé par la loi.

c) Journalisation

Les autorités compétentes doivent tenir un journal des opérations de traitement qu'elles effectuent dans des systèmes de traitement automatisés. Des journaux doivent être tenus à tout le moins pour la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement de données à caractère personnel[212].

La Directive prévoit que les journaux des opérations de consultation et de communication doivent permettre d'établir les motifs, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a

[209] Article relatif à la sécurité du traitement en particulier celui des données sensibles.
[210] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 23 paragraphe 1er.
[211] Ibidem, article 23 paragraphe 3.
[212] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, article 25 paragraphe 1.

consulté le système ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires des données à caractère personnel. Les journaux sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'auto-contrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins de procédures pénales[213].

Lors de ses visites sur site auprès de la Police, la CNPD a constaté l'existence de fichiers de journalisation au niveau du fichier central. Cependant, la CNPD se doit de constater que les mécanismes de journalisation ne permettent pas d'atteindre en pratique l'intégralité des finalités tels qu'énoncés dans la loi. Ainsi, la vérification de la licéité de chaque consultation semble difficile sur base des informations contextuelles limitées qui sont reprises dans le journal (i.e. seul une motivation générique sommaire est reprise dans le journal). Aussi, vu que la pratique courante consiste à ce que les policiers sur le terrain n'accèdent pas directement au fichier, mais font plutôt appel à des policiers au niveau du RIFO, l'identification de la personne qui a in fine consulté le système ne peut pas être retracé de manière systématique avec des efforts raisonnables.

d) L'analyse d'impact et la consultation préalable de l'autorité de contrôle compétente

La loi de transposition impose un exercice nouveau, à savoir la réalisation d'une analyse de l'impact que les opérations de traitement envisagées ont sur les personnes concernées. Une telle analyse s'effectue a priori avant que ledit traitement ne soit mis en place[214].

Il est admis que chaque analyse doit être réévaluée, soit lorsque des changements importants affectant le traitement ont eu lieu, soit au moins tous les trois ans, afin de vérifier son adéquation avec des éventuels changements organisationnels ou techniques qui seraient intervenus entretemps.

La Police devra consulter la CNPD lorsque l'analyse d'impact indique que le traitement présente un risque élevé pour les droits et libertés des personnes concernées qui ne peut être mitigé à travers des mesures organisationnelles et techniques. La CNPD constate que jusqu'à présent, elle n'a pas été consultée en ce qui concerne le fichier central.

Vu l'entrée en vigueur de la loi de transposition, une telle analyse est obligatoire au plus tard pour l'année 2021, ou avant en cas de changements majeurs sur le traitement.

2) La sécurité des données que le responsable du traitement doit garantir

La Directive[215] oblige le responsable du traitement à garantir la sécurité des données à travers la sécurisation des traitements. En effet, elle dispose qu'il est important que « les données à caractère personnel soient traitées de manière à garantir un niveau de sécurité et de confidentialité approprié, notamment en empêchant l'accès non autorisé à ces données et à l'équipement servant à leur traitement ainsi que l'utilisation non autorisée de ces

[213] *Ibidem,* article 25, paragraphe 2.
[214] *Ibidem,* article 26 paragraphe 1.
[215] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO L 119, 4.5.2016, p. 89–131*, article 29.

données et de cet équipement et à tenir compte de l'état des connaissances et de la technologie disponible, des coûts de mise en œuvre au regard des risques et de la nature des données à caractère personnel à protéger »[216].

La loi de transposition impose 10 types de contrôles et de garanties[217] que le responsable du traitement doit mettre en œuvre à la suite d'une évaluation des risques que le traitement peut avoir sur les droits et les libertés des personnes concernées. Il s'agit du contrôle de l'accès aux installations, du contrôle des supports de données, du contrôle de la conservation, du contrôle des utilisateurs, du contrôle de l'accès aux données, du contrôle de la transmission, du contrôle de l'introduction, du contrôle du transport, de la garantie de la restauration et in fine de la garantie de la fiabilité du système et de son intégrité.

Une analyse plus approfondie quant à la sécurité conférée par la Police aux données à caractère personnel traitées via le fichier central permettrait d'avoir une idée plus précise quant à l'observation de ladite obligation. L'objectif de cet avis n'est toutefois pas d'effectuer un audit dédié du volet « sécurité ». Néanmoins, pendant les travaux préparatoires au présent avis certains points d'attention relatifs à ce dernier volet ont été soulevés par la CNPD et communiqués à la Police.

3) Le délégué à la protection des données

La Directive confie au responsable du traitement la désignation d'un délégué à la protection des données (ci-après désigné « le délégué »), *« qui l'aiderait à vérifier le respect au niveau interne, des dispositions adoptées en vertu de la présente directive »*[218]. Cette fonction est nouvelle et s'intègre dans le principe de responsabilisation du responsable du traitement inhérent au RGPD et la Directive.

La loi de transposition prévoit ladite obligation[219] en précisant les qualités professionnelles[220] et l'obligation de publier les coordonnées du délégué à la protection des données[221]. Elle prévoit également la fonction du délégué à la protection des données, ainsi que les missions de ce dernier. A cet égard, il y a lieu de rappeler que le délégué à la protection des données à caractère personnel se doit d'informer et de conseiller le responsable du traitement et les employés, en l'espèce, la Police représentée par son Directeur général quant aux obligations qui leur incombent en tenant compte tant du droit de l'Union que du droit luxembourgeois[222].

Il revient audit délégué de contrôler le respect de la loi de transposition, du droit de l'Union européenne et le droit national par la Police[223].

Le délégué est également tenu de coopérer avec l'autorité de contrôle compétente et faire office de point de contact pour celle-ci et pour les personnes concernées.

[216] *Ibidem,* considérant 28.
[217] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 28 paragraphe 2.
[218] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JO L 119, 4.5.2016, p. 89–131,* considérant 63. Voir également les articles 32 à 34 de la directive.
[219] Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale, article 31 paragraphe 1er.
[220] *Ibidem,* paragraphe 2.
[221] *Ibidem,* paragraphe 4.
[222] *Ibidem,* article 33, paragraphe 1er.
[223] *Ibidem,* paragraphe 2.

La CNPD constate que la Police a désigné un délégué à la protection des données et a rendu public les coordonnées de ce dernier et que celui-ci a été associé aux dossiers ayant trait au traitement des données effectué par la Police via le fichier central.

Il y a à présent lieu d'analyser la qualité du cadre légal encadrant le fichier central.

II. L'analyse de la qualité du cadre légal encadrant le fichier central

Le respect des droits fondamentaux n'est pas absolu puisqu'une ingérence dans ces derniers est reconnue à l'article 52 paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne (ci-après désignée « la Charte »). En effet, cet article dispose que *« toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi »*[224]. La Convention européenne des Droits de l'Homme (ci-après désignée CEDH) quant à elle, rend également possible ladite limitation tout en la rattachant au respect de la vie privée et familiale par exemple[225]. L'importance de prévoir par une loi l'ingérence dans les droits fondamentaux et les libertés est également reprise par la jurisprudence abondante des Hautes juridictions européennes[226].

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 encadre l'ingérence dans les droits et les libertés des individus occasionnée par le traitement mis en œuvre par la Police *via* le fichier central. Néanmoins, cette dernière ne peut pas uniquement se contenter de prévoir l'ingérence faite dans les droits fondamentaux et les libertés par la Police en matière pénale. Elle doit également faire preuve de qualité, conformément à la jurisprudence européenne.

La loi de transposition n'est pas la seule à encadrer légalement le fichier central et le traitement qui en résulte par la Police. Comme précédemment mentionné, la loi du 18 juillet 2018 sur la Police prévoit et encadre les missions de cette dernière qui s'inscrivent incontestablement dans le champ d'application de l'article 1er de la loi de transposition. L'existence du fichier central peut donc être qualifiée de licite dans la mesure où les traitements y effectués sont nécessaires à l'exécution des missions de la Police.

Découlant des besoins liés aux missions de la Police telles que décrites dans sa loi organique, le fichier central est étroitement encadré par la Directive et la loi de transposition très généreuse tant dans sa définition et son interprétation concernant les finalités d'un traitement tombant dans son champ de compétence, que lors de la répartition des prérogatives du responsable du traitement. Sans maintenant s'attarder sur l'analyse de la transposition conforme de la Directive en droit national, on peut tout de même se poser des questions quant à la prise en compte des principes généraux de la matière tels que dégagés par les conventions signées sous l'égide du Conseil de l'Europe

[224] *J.O.U.E.*, C 326, 26.10.2012, p.391-407.
[225] Article 8 paragraphe 2 de la Convention européenne des droits de l'Homme, signée à Rome, le 4.XI.1950.
[226] Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :201 :2014 :238, point 38 ; Avis 1/15, du 8 septembre 2016, EU :C :2016 :656, Cour EDH, Kopp c. Suisse, n° 23224/94, 25 mars 1998, para. 56 à 61; Cour EDH, Amann c. Suisse [GC], n° 27798/95, 16 février 2000, para. 46 à 54; Cour EDH, Brunet c. France, n°21010, 18 décembre 2014, para.35.

et de la jurisprudence de la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne d'une part, ainsi que des principes constitutionnels d'autre part.

La qualité de la loi en matière pénale, s'apprécie au regard du respect du principe de légalité des incriminations. En effet, la légalité des peines est l'énonciation dans la loi des comportements incriminés[227]. Elle a pour effet d' *« assurer la meilleure connaissance possible de la loi pénale ; favoriser la prévisibilité et la sécurité dans les échanges sociaux »*[228], garantir le principe de la hiérarchie des normes et de la séparation des pouvoirs et par là, limiter l'arbitraire du juge. A l'échelle supra nationale, ce principe est consacré par la CEDH à son article 7 qui le perçoit comme un droit absolu auquel nul ne peut déroger[229]. La qualité de la loi est considérée comme un principe général du droit de l'Union européenne[230].

La partie suivante a pour objet d'analyser la qualité du cadre légal encadrant le fichier central géré et exploité par la Police grand-ducale d'une part (A) et de comparer le cadre légal national à celui d'autres États-membres d'autre part (B).

A. <u>La qualité du cadre légal au regard du respect des principes généraux relatifs au traitement des données à caractère personnel en matière pénale</u>

A titre liminaire, il y a lieu de rappeler que la Directive prévoit des conditions de licéité du traitement effectué par les autorités compétentes en matière pénale et en matière de sécurité nationale. En effet, elle dispose que pour être licite, le traitement doit être nécessaire à l'exécution d'une mission de l'autorité compétente, correspondre aux finalités pour lesquelles il a été mis en place mais aussi et surtout, il doit être prévu soit par le droit de l'Union, soit par le droit d'un État-membre[231]. En outre, la Directive précise que la disposition nationale qui réglemente ledit traitement doit au moins préciser : les objectifs du traitement, les données à caractère personnel devant faire l'objet du traitement et les finalités du traitement[232].

Le Règlement général sur la protection des données, pour sa part, dispose également que le fondement du traitement quant 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 est défini par le droit de l'Union ou le droit de l'État-membre auquel le responsable du traitement est soumis[233].

Afin d'analyser au mieux la disposition nationale relative au principe de licéité du traitement et dans le souci d'être le plus précis possible, l'article 7 paragraphe 1er de la loi transposant la Directive peut ici être cité. Il dispose que :

« Le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution des missions de l'autorité compétente définie à l'article 2 paragraphe 1er point 7°, pour une des finalités énoncées à l'article 1er et lorsque cette mission est effectuée en application de disposition législatives régissant l'autorité compétente visée ».

[227] Beccaria, C., (1870). Des délits et des peines. Guillaumin.
[228] Cartuyvels Y., « Les paradigmes du droit pénal moderne en période « postmoderne » : évolutions et transformations, *in* Massé M., J-P. Jean, Giudicelli A. (sous la dir), (2009). Un droit pénal postmoderne ? Mise en perspective des évolutions et ruptures contemporaines. Presses universitaires de France, p. 77.
[229] Cartuyvels Y., Guillain C., Kerchove M., Tulkens F. (Ed.), (2010), *Introduction au droit pénal. Aspects juridiques et criminologiques,* Bruxelles, Kluwer, p. 225.
[230] Traité sur l'Union européenne, J.O.U.E., C 326, 26.10.2012, p. 13-390, article 6 paragraphe 3.
[231] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, article 8 paragraphe 1.
[232] *Ibidem,* article 8 paragraphe 2.
[233] 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), article 6, paragraphe 1, point e, paragraphe 3, point b.

En l'espèce, il ne fait pas de doute que la gestion et l'exploitation du fichier central s'inscrivent dans les missions de la Police telles qu'elles sont prévues par la loi du 18 juillet 2018 sur la Police grand-ducale.

Si la loi du 18 juillet 2018 sur la Police grand-ducale contient un chapitre spécifiquement dédié au traitement de données à caractère personnel, ledit chapitre n'encadre que l'accès par la Police aux fichiers d'autres administrations tels qu'entre autres « le fichier des étrangers exploité pour le compte du Service de étrangers du ministre ayant l'Immigration dans ses attributions »[234], « le fichier des armes prohibées du ministre ayant la Justice dans ses attributions »[235] ou encore « le fichier des sociétés du registre de commerce et des sociétés »[236]. En effet, la CNPD regrette que ledit chapitre ne prévoit pas une disposition relative au traitement de données à caractère personnel dans le cadre de la gestion et de l'exploitation de fichiers par la Police elle-même. Ladite loi ne précise pas non plus que les conditions et modalités d'un tel traitement de données à caractère personnel par la Police puisse faire l'objet d'un règlement grand-ducal.

Il ne revient pas non plus à la loi de transposition de prévoir expressément ledit traitement. En effet, cette loi a pour objet de garantir la protection des données en matière pénale et en matière de sécurité nationale. Il s'agit d'une loi-cadre qui prévoit des règles générales applicables aux autorités compétentes en la matière. Elle n'est pas spécifiquement dédiée à la gestion et à l'exploitation de fichiers par la Police.

Pour répondre aux critères de la jurisprudence européenne, le traitement des données à caractère personnel contenues dans le fichier central doit répondre à des finalités déterminées, explicites et légitimes. Or, les finalités spécifiques du fichier central, explicitement définies et accessibles aux citoyens ne sont ni inscrites dans une notice d'information quant au fonctionnement de ce dernier ni dans la loi du 18 juillet 2018 sur la Police grand-ducale, alors qu'en vertu des dispositions de la loi de transposition le responsable du traitement, en l'espèce la Police grand-ducale représentée par son Directeur général, doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément à cette loi[237]. Il peut être ajouté qu'il ne revient pas non plus à la loi transposant la Directive de préciser les finalités de tous les traitements entrant dans son champ d'application dont fait partie le fichier central.

Dans l'esprit du changement de paradigme au niveau du contrôle de la conformité en matière de protection des données, le législateur national peut certes déléguer des responsabilités importantes au responsable du traitement, encore faut-il que ce dernier les embrasse pleinement. Seul le respect de ses obligations par le responsable du traitement permet de garantir le respect des droits des personnes concernées.

Afin de remplir les critères d'accessibilité et de prévisibilité de la loi, d'une part, et ainsi limiter d'éventuels comportements arbitraires et abusifs de la part de l'autorité compétente, d'autre part, le droit national peut prévoir et encadrer plus spécifiquement la gestion et l'exploitation de fichiers par la Police. C'est la raison pour laquelle, la Cour européenne des droits de l'homme au sein de sa jurisprudence affirme que *« le droit interne doit offrir*

[234] Loi du 18 juillet sur la Police Grand-ducale, article 43 point 3°.
[235] *Ibidem,* point 10.
[236] *Ibidem,* point 11.

une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par l'article 8 paragraphe 1 »[238]. Par conséquent, la loi *« doit définir l'étendue et les modalités d'exercice du pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire »*[239]. La Cour de justice de l'Union européenne estime qu'en cas de limitation de la protection des données à caractère personnel ou du droit au respect de la vie privée un texte légal *« doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »*[240].

Dans la réponse à la question parlementaire n°752, Messieurs les Ministres précisent que la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale constitue la base légale du fichier central.

Ceci étant dit, la CNPD souhaite attirer l'attention sur le fait que le droit national prévoit et encadre l'utilisation de données spécifiques tel que les profils ADN[241], les données collectées dans le cadre du contrôle de l'acquisition et de la détention d'armes[242] ou encore les données contenues dans les dossiers passagers[243]. Le fait d'encadrer le fichier central davantage légalement, ne constituerait donc pas un précédent en la matière pour le législateur luxembourgeois. Si de l'avis de la CNPD, il ne s'agit pas de pallier à une absence de base légale quant à la licéité du fichier central, il n'en reste pas moins qu'une précision législative plus spécifique quant aux finalités précises et quant aux conditions et modalités de gestion et d'exploitation du fichier central contribuerait indiscutablement à améliorer la qualité de la loi.

Une telle précision répondrait aux exigences de la jurisprudence de la Cour constitutionnelle selon laquelle *« dans les matières réservées par la Constitution à la loi, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc »*. Il ne fait aucun doute que les traitements de données effectuées par les autorités compétentes en matière pénale ainsi qu'en matière de sécurité nationale constituent une ingérence dans le droit au respect de la vie privée et le droit à la protection des données, de sorte que les conditions et les modalités de ces traitements doivent obligatoirement être prévues dans la loi. Comme déjà soulevé, le législateur luxembourgeois a opté pour une approche très large de responsabilisation du responsable du traitement aux termes de la loi de transposition. Au regard de l'article 1.3 de la Directive, la CNPD estime qu'un encadrement légal plus strict des obligations de ce dernier augmenterait la qualité de la loi et par là, les garanties pour les personnes concernées.

[238] *Cour EDH,* Amann c. Suisse [GC], n°27798/95 para 56.
[239] *Ibidem.* Voir également Cour EDH, Malone c. Royaume-Uni, série A n°82, du 2 août 1984, pp. 31-32, para.66 ; Cour EDH, Fernández Martínez c. Espagne CE:ECHR:2014:0612JUD005603007, 12 juin 2014 para.117 ; Cour EDH, Liberty et autres c. Royaume-Uni, no 58243/00, du 1er juillet 2008, para. 62 et 63; Cour EDH, Rotaru c. Roumanie, App. N° 28341/95, 4 mai 2000, para. 57 à 59 et Cour EDH, S et Marper c. Royaume-Uni, Requêtes n°30562/04 et 30566/04, du 4 décembre 2008 para. 99. ; Dimitrov-Kazakov c. Bulgarie n°11379/03, du 10 février 2011.
[240] Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :2014 :238, point 54.
[241] Loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle, articles 5 et suivants.
[242] Loi modifiée du 25 mars 1983 sur les armes et munitions, article 5 alinéa 4 qui sera prochainement abrogée. Voir à ce titre le projet de loi n°7425 portant : 1° transposition de la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes ; 2° modification du Code pénal, et 3° abrogation de la loi du 20 avril 1881 concernant le transport et le commerce des matières explosives. Il peut être utile de noter que dans son avis du 8 juillet 2019 relatif au projet de loi précité, la CNPD souligne que ledit projet de loi doit faire preuve de plus de précisions quant à certains éléments relatifs au traitement de données effectué via le fichier armes qui remplacera son prédécesseur à savoir le fichier armes prohibées et autorisations. La CNPD vient ici encore mettre en exergue l'importance de la qualité de la loi.
[243] Loi du 1er août 2018 relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave et portant modification de la loi du 5 juillet portant réorganisation du Service de renseignement de l'État.

Il en va de même de certains autres aspects de ce fichier comme les délais de conservation, la procédure d'accès restreinte à certaines données ou encore des garanties spécifiques destinées au traitement de données à caractère personnel relatives aux personnes physiques vulnérables, en particulier les enfants.

Le législateur luxembourgeois pourrait ainsi utilement faire usage de la faculté laissée aux États-membres telle que prévue au prédit article 1.3 qui dispose que : *« La présente directive n'empêche pas les États-membres de prévoir des garanties plus étendues que celles établies dans la présente directive pour la protection des droits et libertés de personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes ».* Par l'adoption de la Directive, le législateur européen a procédé à une harmonisation minimale des règles applicable en la matière au niveau de l'Union européenne et les États-membres ont la faculté de préciser davantage les règles dans leurs législations nationales respectives tout en respectant le cadre tracé par la Directive.

Rappelons que les précisions proposées ne s'inscriraient en principe pas dans la loi de transposition de la Directive, mais dans les lois spécifiques comme celle sur la Police ou celle relative à la protection de la jeunesse.

L'examen des dispositions relatives aux traitements de données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale dans les législations des pays voisins peut être utile et peut servir d'exemple au législateur luxembourgeois.

B. Le cadre légal national comparé à celui d'autres États-membres en la matière

1) Situation générale

Avant de faire état des législations nationales des pays qui entourent le Luxembourg, rappelons que la CNPD a sollicité les autorités de la protection des données de l'ensemble des États-membres de l'Union européenne afin de savoir si la loi transposant la Directive sert de base légale au traitement effectué par la Police à travers leurs fichiers ou si des lois ou des dispositions règlementaires spécifiquement dédiées à la gestion, à l'exploitation et à l'utilisation de fichiers policiers ont été adoptées. Sur les 25 réponses obtenues, dont il faut retirer les deux États-membres qui n'avaient pas encore adopté de loi de transposition au moment où la CNPD a effectué son sondage, et deux dont la réponse ne permet pas de déterminer sans ambiguïté leur situation, seulement cinq affirmaient que la loi de transposition servait de base légale au traitement effectué par les fichiers de la Police. Par contre, 16 États-membres ont affirmé disposer de textes spécifiquement dédiés. Les pays voisins au Luxembourg font partis de ce dernier groupe, puisqu'ils prévoient un encadrement légal spécifiquement dédié aux fichiers exploités par la Police.

En France par exemple, la loi transposant la Directive en droit national prévoit explicitement l'encadrement par disposition législative ou réglementaire tout traitement de données à caractère personnel en matière pénale[244]. Dans un rapport du 17 octobre 2018, il est fait état de l'effort de régularisation des nombreux fichiers de la police[245] en France, si bien que la Commission Nationale de l'Informatique et des Libertés (CNIL) estimait à cette date qu'il n'y a plus de fichiers de police irréguliers puisque ces derniers disposent d'une base légale qui leur est propre[246]. En plus de l'existence d'une base légale ou réglementaire sur laquelle reposent les fichiers gérés et exploités par la police, les finalités desdits fichiers y sont précisées. A titre d'exemple, il est précisé dans la fiche descriptive du fichier TAJ que *« Le traitement d'antécédents judiciaire (TAJ), en application des articles 230-6 à 230-11 du Code de procédure pénale, est utilisé dans le cadre des enquêtes judiciaires (recherche des auteurs d'infractions) et d'enquêtes administratives (comme les enquêtes préalables à certains emplois publics ou sensibles) »*[247].

En Belgique, la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel met en œuvre le RGPD et transpose la Directive en droit national. Cette loi prévoit également la nécessité d'une base légale spécifique à savoir un texte légal ou réglementaire encadrant les traitements de données à caractère personnel en matière pénale[248]. Dans la lignée du législateur français, le législateur belge dote les fichiers de la police de bases légales spécifiques. En effet, la loi sur la fonction de police dispose que *« lorsque l'exercice des missions de police administrative et de police judiciaire nécessite que les services de police structurent les données à caractère personnel et les informations visées à l'article 44/1 de sorte qu'elles puissent être directement retrouvées, celles-ci sont traitées dans une banque de données policière opérationnelle [..] »*[249]. La loi encadre trois types de fichiers à savoir « la Banque de données Nationale Générale », « les banques de données de base », « les banques de données particulières ». La loi belge précise également les finalités de ces trois types de banques de données. A titre d'exemple, la Banque de données Nationale Générale est utilisée par les services de police belge pour exercer leurs missions afin de permettre : « l'identification des personnes visées à l'article 44/5, paragraphe 1er et 3 ; l'identification des personnes ayant accès à la B.N.G. ; la coordination et le croisement des données à caractère personnel et informations policières ; la vérification au niveau national des antécédents de police administrative et de police judiciaire ; l'aide aux contrôles effectués par les services de police par l'indication des mesures à prendre soit sur la base d'une décision des autorités de police administrative ou des autorités de police judiciaire compétentes, soit en fonction de l'existence des antécédents de police administrative ou de police judiciaire ; l'appui à la définition et à la réalisation de la politique policière et de sécurité »[250].

En Allemagne in fine, les fichiers gérés et exploités par la police sont principalement réglés au niveau des Länder[251]. Par exemple, dans le Land de Hesse, ce sont la loi de police ainsi que des règlements d'application de cette loi qui prévoient la mise en place d'un système de consultation automatisé des données policières[252].

[244] La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifiée), articles 88 et 89.
[245] En 2009, il existait en France 58 bases de données gérées et exploitées par la police et 27% d'entre elles étaient dénuées de bases légales. N°1548 Assemblée Nationale, Constitution du 4 octobre 1958, treizième législature, enregistré à la Présidence de l'Assemblée nationale le 24 mars 2009. Rapport d'information déposé en application de l'article 145 du Règlement par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers de police. Par Mme Delphine BATHO et M. Jacques Alain BENISTI, Députés, p. 43 et suivantes.
[246] N°1335 Assemblée Nationale, Constitution du 4 octobre 1958, Quinzième législature, enregistré à la Présidence de l'Assemblée nationale le 17 octobre 2018, Rapport d'information déposé en application de l'article 145 du Règlement par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur les fichiers mis à la disposition des forces de sécurité et présenté par MM. Didier PARIS et Pierre MOREL-A-L'HUISSIER, Députés, p.9.
[247] Fiche descriptive du fichier « TAJ : Traitement d'Antécédents judiciaires » disponible sur la page https://www.service-public.fr/particuliers/vosdroits/F32727, consultée pour la dernière fois le 24/08/2019.
[248] 30 juillet 2018 loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Titre 2., article 33 paragraphe 1er.
[249] 5 août 1992 loi relative sur la fonction de police (mise à jour au 19-06-2019), article 44/2 paragraphe 1er.
[250] *Ibidem*, article 44/7.
[251] Il existe toutefois des traitements de données (traitements à caractère national et échanges de données) réglés au niveau fédéral, surtout dans la loi BKA, Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten.
[252] Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG), voir également Verordnung zur Durchführung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Hessischen Freiwilligen-Polizeidienst-Gesetzes (HSOG-DVO) vom 12. Juni 2007.

Il est donc indéniable que les législations des pays voisins prévoient la gestion et l'exploitation des fichiers par la police et en précisent les finalités.

2) La question des dispositions spécifiques relatives aux délais de conservation des données

Comme mentionné précédemment, le responsable du traitement se doit notamment de fixer les délais appropriés pour l'effacement des données à caractère personnel et l'établissement de règles procédurales en vue du respect desdits délais. La CNPD se demande s'il est opportun de confier de telles responsabilités au Directeur général de la Police grand-ducale. En effet, une telle marge de manœuvre est susceptible de méconnaître les principes d'accessibilité et de prévisibilité de la loi qui découlent du principe de légalité de la loi pénale. A cet égard, la Cour européenne des droits de l'homme au sein de sa jurisprudence affirme que *« le droit interne doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par l'article 8 paragraphe 1*[253] *»*[254]. Par conséquent, la loi *« doit définir l'étendue et les modalités d'exercice du pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire »*[255].

Dans les législations des pays voisins, les délais de conservation des données à caractère personnel au sein des fichiers gérés et exploités par la police sont fixés dans des base légales dédiées spécifiquement à ces fichiers en question.

En France par exemple, la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation de la performance de la sécurité intérieure qui encadre le fichier relatif au traitement d'antécédents judiciaires[256] dispose que les données concernant les personnes mises en cause majeures sont conservées 20 ans. Les données concernant les personnes mineures mises en cause sont conservées 5 ans et les données concernant les victimes sont conservées au maximum 15 ans[257]. Un tel exemple révèle le degré de précision de la loi française énonçant explicitement les délais de conservation des données tout en effectuant la distinction entre les différentes catégories de personnes concernées.

En Belgique, la loi sur la fonction de police prévoit que les données traitées dans la Banque de données Nationale Générale à des fins de police judiciaire sont archivées lorsqu'elles présentent un caractère non adéquat, non pertinent ou excessif. L'archivage s'effectue un an à partir de l'enregistrement du fait s'il s'agit d'un fait qualifié de contravention, dix ans s'il s'agit d'un fait qualifié de délit et trente ans s'il s'agit d'un fait qualifié de crime, à partir de l'enregistrement du fait[258]. La durée de l'archivage est de 30 ans. A l'expiration de ces 30 ans, les données sont effacées[259].

[253] Convention européenne des droits de l'homme.
[254] Cour EDH, Amann c. Suisse [GC], n°27798/95 para 56.
[255] *Ibidem.* Voir également Cour EDH, Malone c. Royaume-Uni, série A n°82, du 2 août 1984, pp. 31-32, para.66 ; Cour EDH, Fernández Martínez c. Espagne CE:ECHR:2014:0612JUD005603007, 12 juin 2014 para.117 ; Cour EDH, Liberty et autres c. Royaume-Uni, no 58243/00, du 1er juillet 2008, para. 62 et 63; Cour EDH, Rotaru c. Roumanie, App. N° 28341/95, 4 mai 2000, para. 57 à 59 et Cour EDH, S et Marper c. Royaume-Uni, Requêtes n°30562/04 et 30566/04, du 4 décembre 2008 para. 99. ; Dimitrov-Kazakov c. Bulgarie n°11379/03, du 10 février 2011.
[256] Le traitement d'antécédents judiciaire (TAJ) est un fichier commun à la police et à la gendarmerie nationale, en remplacement des fichiers STIC de la police nationale et JUDEX, de la gendarmerie nationale, qui ont été définitivement supprimés.
[257] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, voir également les articles 230-6 à 230-11 du Code de procédure pénale.
[258] 5 août 1992 loi relative sur la fonction de police (mise à jour au 19-06-2019), article 44/9 et suivants.
[259] *Ibidem,* article 44/10.

En Allemagne, les Länder prévoient également des délais de conservation et d'archivage des données à caractère personnel contenues dans les fichiers de la police. C'est le cas notamment du Land de Hesse dont le règlement d'exécution de la loi de police dispose que la nécessité de conserver les données doit être appréciée de manière régulière et qu'une vérification de la pertinence de la conservation doit avoir lieu tous les 10 ans. Les délais de conservation sont également modulés en fonction de ce qu'il s'agit d'une personne physique mineure ou majeure.

Au vu des présentes considérations, la CNPD estime que les délais de conservation ou du moins les critères applicables pour déterminer la durée de conservation ainsi que les procédures permettant la vérification régulière de la nécessité lesdits délais mériteraient d'être précisés par le législateur afin de limiter au maximum la marge de manœuvre du responsable du traitement et garantir la transparence, l'accessibilité et la proportionnalité desdits délais.

3) La question des dispositions spécifiques relatives aux personnes vulnérables et aux données sensibles

Aux termes de ses considérants, la Directive prévoit que *« les mesures prises par le responsable du traitement devraient comprendre l'établissement et la mise en œuvre de garanties spécifiques destinées au traitement de données à caractère personnel relatives aux personnes physiques vulnérables, telles que les enfants »*[260].

Dans son corps de texte, la Directive ne prévoit pas de dispositions particulières relatives aux traitements des données à caractère personnelles des personnes mineurs par les responsables de traitement qu'elle vise, tout comme la loi de transposition se retreint de le faire.

La loi du 10 août 1992 relative à la protection de la jeunesse ne fait pas non plus état d'une telle protection.

La législation luxembourgeoise diffère donc également à cet égard si on la compare avec celles des pays voisins. En effet, la France et l'Allemagne prévoient des garanties spécifiques au traitement des données à caractère personnel des personnes mineures lorsque celles-ci sont contenues au sein de fichiers policiers[261].

Conclusion

Le traitement des données à caractère personnel tel qu'effectué par la Police grand-ducale à travers le fichier central est encadré 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 et par la loi du 18 juillet 2018 sur la Police grand-ducale qui prévoit explicitement les missions de cette dernière. Ensemble, ces deux lois confèrent un fondement légal et rendent licite le traitement de données relatif au fichier central.

[260] Directive, considérant 50.
[261] Voir en ce sens les développements effectués dans le point précédent.

L'utilisation du fichier central soulève toutefois un certain nombre de questions quant à la conformité du traitement aux dispositions de la loi de transposition.

Dans l'esprit du changement de paradigme en matière de contrôle dans le domaine de la protection des données, le législateur a chargé le responsable du traitement en matière de pénale et de sécurité nationale du respect des obligations de la loi. Il lui appartient de définir les politiques appropriées en matière de protection des données et de mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer à tout moment que le traitement est effectué conformément à la loi de transposition.

Pour ce qui est du fichier central, il est incontestable que la Police grand-ducale en tant que responsable du traitement n'est actuellement pas en mesure de démontrer pleinement cette conformité, ce qui met en péril la garantie des droits et libertés des personnes concernées, ainsi que la confiance que portent les citoyens en cette institution importante.

Cette situation de fait amène la CNPD à conclure que la situation actuelle nécessite une intervention qui va au-delà du périmètre strict de la Police grand-ducale afin de garantir une protection effective des droits des personnes concernées.

Dans cette perspective et afin de mieux encadrer les obligations du responsable du traitement en l'espèce et de façon générale pour améliorer la qualité de loi encadrant la matière, la CNPD propose que le législateur précise la législation nationale à cet égard, en vertu de l'article 1.3 de la Directive et à la lumière de la jurisprudence des Hautes juridictions européennes.

Ainsi, la loi sur la Police devrait être complétée de dispositions précisant, entre autres, le principe et les finalités spécifiques des fichiers opérés par la Police grand-ducale pour les besoins d'exécution de ses missions, les délais de conservation des données ou les critères applicables pour déterminer les durées de conservation des données, ainsi que les autres aspects essentiels des traitements de données opérés par la Police grand-ducale, tels que développés plus haut dans le présent avis.

Partant, les mesures législatives à adopter devraient préciser le cadre législatif général posé par la loi de transposition quant aux aspects essentiels des traitements de données, mais aussi prévoir la possibilité d'adopter des règlements grand-ducaux pour régler les modalités moins essentielles, à la lumière de la jurisprudence de la Cour constitutionnelle.

Entre-temps, la Commission nationale fait appel à la Police grand-ducale de se conformer le plus rapidement possible aux obligations résultant de la loi de transposition de la Directive (UE) 2016/680 et plus particulièrement au niveau des points suivants :

- Etablir la documentation complète relative au fichier central précisant tant l'objet que les finalités spécifiques de ce dernier, ainsi que les mesures techniques et organisationnelles adoptées compte tenu de la nature, de la portée, du contexte des finalités du traitement ainsi que des risques.

- Revoir les accès au fichier central accordés au regard de leur nécessité alors qu'à l'heure actuelle, il semble y avoir un décalage entre le nombre important des accès accordés au fichier central et l'utilisation effective de ces accès.

Mettre en place une journalisation conforme à l'article 24 de la loi de transposition et plus particulièrement de :

- prendre des mesures permettant de garantir que l'identité de la personne ayant fait une demande de recherche (en particulier par téléphone) puisse être retracée dans le cas de figure où un agent effectue pour le compte d'un autre la recherche dans le fichier central ;

- assurer la tenue des journaux conformément aux règles de la loi de transposition.

- Fixer sans ambiguïté les délais de conservation appropriés et établir des règles procédurales en vue d'assurer le respect de ces délais et plus particulièrement :

  - améliorer la transparence et la précision quant aux délais de conservation ;

  - vérifier l'adéquation du délai de conservation de la partie active au regard des délais de prescription applicables ;

  - vérifier le caractère proportionné de la durée de conservation de la partie archives.

Convaincue qu'une amélioration de la protection des droits des personnes concernées pourra en résulter, la Commission nationale salue la coopération de la Police grand-ducale et du Ministère Public en vue de la mise en place d'un système de transmission automatisé d'informations succinctes sur le suivi réservé par les autorités judiciaires aux procès-verbaux transmis par la Police grand-ducale et encourage les protagonistes de faire avancer rapidement leurs travaux.

Entre-temps et afin que les droits et libertés des personnes concernées, dont les données figurent dans le fichier central, soient garanties, la CNPD estime nécessaire de mettre en place un mécanisme de transmission manuel entre les autorités judiciaires et la Police grand-ducale, afin que cette dernière soit en mesure de garantir l'exactitude et la mise à jour des données.

Au regard des éléments dont dispose la CNPD actuellement quant à la structure et la configuration du fichier central, elle tient à rappeler que la Police grand-ducale ne pourra pas se réfuter derrière des contraintes techniques pour justifier une non-conformité. Il incombe à ce moment au responsable du traitement de prendre toutes les mesures nécessaires pour assurer qu'il soit en mesure de respecter pleinement les droits des personnes concernées – même si ceci nécessite le redéveloppement d'un système informatique.

La Commission nationale fait également appel aux autorités compétentes pour soutenir la Police grand-ducale dans ses travaux de mise en conformité, notamment en lui mettant à disposition les ressources nécessaires à cette fin.

Enfin, la Commission nationale suggère aux autorités compétentes de préciser et mettre en œuvre des garanties spécifiques destinées au traitement de données à caractère personnel relatives aux personnes physiques vulnérables telles que les enfants.

Ainsi décidé à Esch-sur-Alzette en date du 13 septembre 2019.

La Commission nationale pour la protection des données

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

ANNEXES

5

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal précisant les modalités de gestion de l'identification des personnes et les catégories de données contenues dans les annuaires référentiels d'identification des patients et des prestataires.

Délibération n°50/2019 du 18 octobre 2019

Conformément à l'article 57 paragraphe (1) lettre (c) du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après désigné « le RGPD »), chaque autorité de contrôle a pour mission de conseiller *« conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement »*. L'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

Par courrier du 26 juillet 2019, Monsieur le Ministre de la Sécurité Sociale a fait parvenir à la Commission nationale une série d'amendements au projet de règlement grand-ducal précisant les modalités de gestion de l'identification des personnes et les catégories de données contenues dans les annuaires référentiels d'identification des patients et des prestataires (ci-après « les amendements »), ainsi qu'un texte coordonné dudit projet de règlement grand-ducal.

Pour rappel, la CNPD a rendu, le 21 décembre 2018[262], un premier avis relatif au projet de règlement grand-ducal précisant les modalités de gestion de l'identification des personnes et les catégories de données contenues dans les annuaires référentiels d'identification des patients et des prestataires (ci-après « le projet de règlement grand-ducal ») dans lequel elle a souligné l'importance de conférer une base légale au dispositif d'identitovigilance développé par l'Agence nationale des informations partagées dans le domaine de la santé (ci-après désignée « l'Agence eSanté ») d'une part, et aux annuaires référentiels d'identification des patients et des prestataires de soins de santé, d'autre part, en permettant de garantir les objectifs de sécurité et de qualité de l'information qui sous-tendent la mise en place desdits outils par l'Agence eSanté. Le Conseil d'État s'était déjà prononcé sur le projet de règlement grand-ducal dans un avis rendu le 27 novembre 2018.

La Commission nationale remarque que certaines de ses observations ont été prises en compte par les auteurs des amendements. Elle entend ainsi limiter ses observations aux amendements du projet de règlement grand-ducal pour lesquels les auteurs n'ont pas suivi les recommandations de la CNPD.

[262] Délibération n°491/2018 du 21 décembre 2018.

Ad amendement 1er

Le nouvel alinéa 4 de l'article 1er du projet de règlement grand-ducal, créé par le point 4 de l'amendement 1er, prévoit toujours la mise en place de règles de traçage des accès à la plateforme électronique nationale d'échange et de partage de données de santé (ci-après : « la plateforme »). Néanmoins, au vu du titre du projet sous avis, qui reste inchangé suite aux amendements nous soumis, la CNPD ne peut que réitérer la position du Conseil d'État exprimée dans son avis du 27 novembre 2018 s'étant demandé si *« la disposition sous revue ne dépasse pas le cadre tracé par l'article 60ter, paragraphe 2, du Code de la sécurité sociale dans la mesure où la plateforme constitue le point d'entrée à plusieurs systèmes de traitement de données dont celui qui fait l'objet du règlement grand-ducal en projet. »*[263] Comme la CNPD l'a relevé dans son avis du 21 décembre 2018, ladite plateforme permet aux professionnels de soins de santé et aux patients d'accéder à un ensemble de services proposés par l'Agence eSanté, comme par exemple le dossier de soins partagé.

En ce qui concerne toujours l'amendement 1er, point 3, visant à créer un nouvel alinéa 3 de l'article 1er du projet de règlement grand-ducal, la CNPD constate qu'en comparant ledit alinéa à sa version initiale (l'ancien article 1er, alinéa 2), il n'est plus prévu que les données de journalisation et de traçabilité doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement et qu'elles soient effacées après (sauf en cas de procédure de contrôle), mais que lesdites données *« régulièrement mises à jour, sont conservées tant que dure la procédure de contrôle »*. La CNPD comprend que cette modification se base sur l'avis du Conseil d'État du 27 novembre 2018 ayant proposé de préciser dans ce contexte *« que les données sont effacées dès que la procédure de contrôle est clôturée et que les données sont régulièrement mises à jour. »*

La CNPD se demande tout d'abord si des procédures de contrôle de l'Agence eSanté et des prestataires intervenant dans la prise en charge des patients ayant accédé ou consulté les annuaires référentiels d'identification des patients et des prestataires de soins de santé sont déclenchées régulièrement, et si oui, par qui et à quel intervalle. Par ailleurs, la CNPD ne saisit pas la portée de cette modification et elle suggère de maintenir une durée de conservation des données de journalisation et de traçabilité de cinq ans à partir de leur enregistrement, tout en tenant compte du fait qu'une éventuelle procédure de contrôle aurait un effet suspensif et les données seraient dès lors à supprimer uniquement lors de la clôture de cette procédure de contrôle. En effet, la finalité de la conservation des logs relatifs aux accès consiste justement à pouvoir vérifier et constater d'éventuels abus que ce soit par l'Agence eSanté ou par le patient.

Finalement, dans le commentaire des articles de la version initiale du projet de règlement grand-ducale il était précisé qu'afin d'identifier les professionnels de santé souhaitant se connecter à la plateforme, l'Agence eSanté attribuerait un identifiant électronique unique à chaque professionnel de santé et collectivité de santé dans le cadre des échanges électroniques à travers la plateforme.

[263] Avis n°CE 53.106 du Conseil d'Etat du 27 novembre 2018.

Or, il n'était pas clair si chaque professionnel de santé travaillant dans une collectivité de santé aurait un identifiant personnel, alors que la CNPD a considéré qu'il n'est pas admissible qu'une telle collectivité dispose d'un identifiant en commun.

La Commission nationale suppose qu'avec l'ajout du nouvel alinéa 2, premier point, cette problématique est résolue et que chaque prestataire de santé aura son identifiant personnel, ledit alinéa précisant que l'identitovigilance vise, entre autres, à *« garantir et certifier l'identité du patient et du prestataire intervenant dans la prise en charge du patient par l'attribution d'un identifiant unique dans chaque annuaire pour chaque identité existante. »* Le commentaire dudit amendement renforce ce constat en soulignant qu'afin de *« garantir cette qualité et sécurité des soins, chaque utilisateur de la plateforme, qu'il soit patient ou prestataire, doit être identifié de manière univoque, c'est-à-dire sans ambiguïté. »*

Ad amendement 3

L'amendement 3 vise à remplacer dans le nouvel article 2, alinéa 2 du projet de règlement grand-ducal les termes « ces données » par « les données contenues dans les annuaires référentiels d'identification ». Par cette modification, l'alinéa 2 en question aura alors la teneur suivante : *« Les données contenues dans les annuaires référentiels d'identification sont conservées pendant au maximum dix ans à compter du jour où l'identification du patient, respectivement du prestataire de soins devient sans objet dans le cadre des traitements de données visés à l'article 60ter du Code de la sécurité sociale et ce sans préjudice des dispositions fixant une durée de conservation particulière des données traitées sur la plateforme électronique nationale d'échange et de partage de données de santé par l'Agence. »*

Quant au fond, le projet de règlement grand-ducal prévoit donc toujours, comme dans sa version initiale, une durée de conservation maximale de 10 ans des données à caractère personnel figurant dans les annuaires référentiels d'identification des patients et des prestataires de soins de santé. Déjà dans son avis du 21 décembre 2018, la Commission nationale a estimé qu'il n'est pas possible de cerner quel est le point de départ exact de ce délai de 10 ans. Elle réitère sa position à cet égard, ainsi que ses remarques générales concernant la durée de conservation de 10 ans :

« Ainsi, pour fixer le déclenchement de la durée de conservation maximale de 10 ans, la CNPD se rallie à l'avis du Conseil d'État ayant recommandé aux auteurs du projet de règlement grand-ducal de s'inspirer des points de départ prévus dans le projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé pour la suppression des données, à savoir le décès du patient et la fermeture des applications de la plateforme. La CNPD estime donc nécessaire de décrire de manière concise dans le corps du texte du projet de règlement grand-ducal sous avis quel est le point de départ exact du délai de 10 ans.

Outre la question du début précis de la période de conservation, la Commission nationale se demande de manière générale si le délai de 10 ans est justifié par rapport aux finalités poursuivies par la mise en place de l'annuaire référentiel d'identification des patients. Les auteurs du projet de loi n°7061 devenu la loi du 13 décembre 2017 modifiant certaines dispositions du Code de la sécurité sociale, décrivaient les finalités dudit annuaire, ainsi que de l'annuaire référentiel d'identification des prestataires de soins de santé de la manière suivante : « Une gestion sécurisée des identités s'impose non seulement pour les accès des patients et des prestataires à la plateforme nationale et au dossier de soins partagé mais, de manière générale, dans tous les projets informatiques à envergure nationale visant un échange sécurisé ou une meilleure utilisation des données relatives à la santé. A cette fin, l'Agence eSanté a mis en place un système de surveillance et de prévention des erreurs et risques liés à l'identification des patients et des prestataires pour gérer la qualité et la fiabilité des informations traitées dans les services déployés. Il est essentiel de garantir qu'un même patient ou prestataire est identifié de manière unique dans tout l'écosystème de la plateforme et dans les communications réciproques avec les systèmes d'informations des acteurs du domaine de la santé et des soins. »[264] *Le commentaire des articles du règlement grand-ducal sous avis précise à cet égard que la durée de conservation vise à s'aligner à la durée maximale pendant laquelle les professionnels et les établissements de santé, utilisant une application de la plateforme pour la gestion de leurs dossiers patients, conservent en pratique les données. Le commentaire continue en ce sens que les « données pourront toutefois être supprimées dans un délai plus court si leur conservation n'est plus justifiée au regard des besoins d'interaction de l'annuaire avec les applications de la plateforme. »*

Or, en considérant que l'annuaire référentiel d'identification des patients ne se substituera pas aux dossiers des patients tenus par les médecins, établissements hospitaliers et autres professionnels de santé, la Commission nationale considère qu'une durée de conservation de dix ans après le décès d'un patient ou la fermeture des applications de la plateforme apparaît comme excessive au regard des finalités précitées dudit annuaire. »

La Commission nationale avait exprimé dans son avis précité les mêmes observations concernant la durée de conservation des données contenues dans les annuaires référentiels d'identification des prestataires de soins de santé.

Ainsi décidé à Esch-sur-Alzette en date du 18 octobre 2019.

La Commission nationale pour la protection des données

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

[264] Commentaire des articles du projet de loi n°7061 modifiant certaines dispositions du Code de la sécurité sociale, déposé le 13 septembre 2016.

ANNEXES

5

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

Délibération n°51/2019 du 18 octobre 2019

Conformément à l'article 57 paragraphe (1) lettre (c) du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après désigné « le RGPD »), chaque autorité de contrôle a pour mission de conseiller *« conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement »*. L'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD.

Par courrier en date du 26 juillet 2019, Monsieur le Ministre de la Sécurité Sociale a fait parvenir à la Commission nationale une série de propositions d'amendements au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé (ci-après « les amendements »), ainsi qu'un texte coordonné dudit projet de règlement grand-ducal.

Pour rappel, la CNPD a rendu, le 5 avril 2018[265], un premier avis relatif au projet de règlement grand-ducal précisant les modalités et conditions de mise en place du dossier de soins partagé (ci-après « le projet de règlement grand-ducal ») dans lequel elle a formulé toute une série d'observations sur les dispositions dudit projet ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel.

Le Conseil d'État quant à lui s'est prononcé sur le projet de règlement grand-ducal dans un avis rendu le 23 octobre 2018, dans lequel il a repris de nombreuses critiques émises par la Commission nationale dans son avis précité du 5 avril 2018.

La Commission nationale se félicite du fait que certaines de ses remarques ont été prises en compte par les auteurs des amendements.

I. Remarques préliminaires

[265] Délibération n°242/2018 du 5 avril 2018.

a. Principe de licéité d'un traitement de données à caractère personnel

Dans son avis du 5 avril 2018, la CNPD a considéré qu'au vu du principe de licéité d'un traitement de données à caractère personnel qui doit être lu à la lumière de l'article 8 paragraphe (2) de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52 paragraphes (1) et (2) de la Charte des droits fondamentaux de l'Union européenne[266], au moins les dispositions concernant la durée de conservation des données au dossier de soins partagé (ci-après : « DSP »), les droits des titulaires mineurs non émancipés et titulaires majeurs protégés par la loi, ainsi que la limitation du droit d'accès et du droit à l'effacement devraient être prévues dans la loi au sens stricte du terme et plus précisément par l'article 60*quater* du Code de la sécurité sociale, et non pas dans un acte réglementaire.

Tout d'abord, la CNPD remarque que les dispositions sur la durée de conservation des données à caractère personnel au DSP sont toujours prévues aux articles 4 et 9 paragraphe (5) du projet de règlement grand-ducal amendé.

Par ailleurs, par l'amendement 7, les auteurs ont supprimé l'article 7 du projet de règlement grand-ducal concernant les titulaires mineurs non émancipés et titulaires majeurs protégés par la loi pour les raisons suivantes : *« Les avis du Conseil d'État et de la Commission nationale pour la protection des données établissent que l'article 7, du moins en partie, déroge aux règles relatives aux mineurs et aux majeurs protégés par la loi telles que prévues au Code civil.*

Ainsi dans un souci du respect de la hiérarchie des normes, l'article 7 est supprimé, les dispositions qui introduisent des droits spécifiques pour certains mineurs devant être reprises dans les lois particulières régissant leurs droits. »

En ce qui concerne une limitation des droits des personnes concernées, comme notamment le droit d'accès, l'article 23 paragraphe (1) du RGPD dispose que le droit de l'Union ou le droit de l'État-membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter, entre autres, la portée du droit d'accès prévu par l'article 15 du RGPD. Une telle limitation doit respecter l'essence des libertés et droits fondamentaux et elle doit constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir un des dix motifs y prévus. Une mesure législative limitative doit d'ailleurs contenir certaines dispositions spécifiques énumérées à l'article 23 paragraphe (2) du RGDP.

Dans son avis du 5 avril 2018, la CNPD avait remarqué que comme l'article 9 paragraphe (2) du projet en sa version initiale limitait le droit d'accès des titulaires, représentants légaux et médecins référents, cette limitation devrait être prévue par une loi au sens stricte du terme et respecter les exigences susmentionnées prévues à l'article 23 du RGPD. Par son amendement 8, les auteurs expliquent que comme le nouvel article 7 paragraphe (4) *« prévoit de rendre inaccessibles au titulaire certaines données pouvant causer le cas échéant un préjudice grave pour sa santé, [il] est supprimé suite à l'avis précité du Conseil d'État vu qu'il restreint les droits d'accès du*

[266] Pour plus de détails, la CNPD renvoie à son avis du 5 avril 2018.

titulaire à son dossier de soins partagés, tels qu'attribués par la base légale qu'est l'article 60quater du Code de la sécurité sociale. »

Hormis les articles concernant la durée de conservation des données, la CNPD constate donc que ses autres recommandations concernant les dispositions pour lesquelles un cadre réglementaire n'est pas suffisant, mais où un encadrement par une loi au sens stricte du terme est requis, ont été prises en compte par les auteurs des amendements du projet de règlement grand-ducal. Or, elle regrette qu'après plus de 17 mois après l'adoption de son avis précité, aucun projet de loi n'ait été déposé à la Chambre des Députés, en vue d'adopter les mesures législatives nécessaires pour prendre en compte lesdites considérations La CNPD profite par ailleurs de l'occasion pour réitérer sa recommandation émise au législateur dans le cadre de son avis du 5 avril 2018 de s'inspirer du Code de la santé publique français afin de prévoir dans la législation luxembourgeoise des sanctions pénales en cas d'abus d'accès au DSP.

b. La question de la responsabilité du traitement

L'article 60*ter* paragraphe (4) du Code de la sécurité sociale prévoit que l'Agence nationale des informations partagées dans le domaine de la santé (ci-après désignée « l'Agence eSanté ») a la qualité de responsable du traitement des données à caractère personnel au sens de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, loi abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données.

Or, la CNPD a déjà estimé à maintes reprises[267] que la responsabilité unique de l'Agence eSanté concernant les traitements des données à caractère personnel contenues dans le DSP ne correspond pas à la réalité tel que le système est envisagé. En effet, il ressort de l'économie générale de la loi du 17 décembre 2010 portant réforme du système de soins de santé que l'Agence eSanté d'un côté, et les professionnels de santé d'autre côté, participent conjointement à la réalisation des finalités et des moyens du traitement tels que définis par le législateur. L'article 26 paragraphe (1) du RGPD exige que *« les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, par voie d'accord entre eux, sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État-membre auquel les responsables du traitement sont soumis. »*

La Cour de Justice de l'Union européenne a pris position à l'égard de la notion de « responsabilité conjointe » dans un arrêt récent en jugeant que son existence *« ne se traduit pas nécessairement par une responsabilité équivalente, pour un même traitement de données à caractère personnel, des différents acteurs. Au contraire, ces acteurs*

[267] Voir la délibération n°345/2010 du 24 novembre 2010 relatif au projet de loi n°6196 portant réforme du système de soins de santé, ainsi que la délibération n°242/2018 du 5 avril 2018 sur le projet de règlement grand-ducal sous examen.

peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce. »[268]

La CNPD constate dans ce contexte que les auteurs des amendements ont pris conscience que ce n'est pas uniquement l'Agence eSanté qui est à considérer comme responsable du traitement, mais que différents acteurs assument différentes responsabilités en ce qui concerne le traitement des données contenues dans le DSP. En effet, le commentaire de l'amendement 8 mentionne les obligations et responsabilités des professionnels de santé intervenant dans la prise en charge médicale du patient leur incombant en vertu de l'article 13 du RGPD, tandis que l'amendement 2 prévoit les obligations et responsabilités de l'Agence eSanté en vertu de l'article 14 du RGPD. Les auteurs expliquent dans ledit commentaire que ces précisions poursuivent *« la même volonté de déterminer clairement les obligations et responsabilités des différents intervenants en vertu de l'article 26 du règlement (UE) 2016/679 comme préconisé par le Conseil d'État et la Commission nationale pour la protection des données dans leurs avis respectifs. »*

Par ailleurs, les paragraphes (3) alinéa 4 et (5) de l'article 6 du texte coordonné du projet de règlement grand-ducal prévoient que le droit à l'effacement, respectivement le droit d'obtenir la rectification des données inexactes ou incomplètes dans son DSP, doivent être exercés soit auprès du professionnel de santé, soit auprès de l'Agence eSanté.

Finalement, dans sa version actuelle, l'article 10 paragraphe (2) du projet de règlement grand-ducal concernant la sécurité de la plateforme mentionne que le prestataire est à considérer comme responsable du traitement et qu'il peut recourir à des sous-traitants afin de mettre en œuvre les mesures techniques et organisationnelles de sécurité appropriées afin de garantir un niveau de sécurité adapté aux risques. Des précisions quant à la notion d'un « prestataire » se retrouvaient dans le commentaire des articles de la version initiale du projet de règlement grand-ducal : *« Vu la diversité des prestataires susceptibles de se connecter à la plateforme ou d'utiliser l'une de ses applications, à savoir un établissement hospitalier, une pharmacie, un laboratoire d'analyses médicales et de biologie clinique, une association de médecins ou un cabinet individuel et, pour les données mentionnées à l'article 60quater, paragraphe 2 du Code de la sécurité sociale, un réseau d'aides et de soins, un centre semi-stationnaire, un établissement d'aides et de soins, un établissement à séjour intermittent […] »*. Or, la CNPD avait recommandé aux auteurs d'ajouter une définition dudit terme à l'article 1er du projet.

Ainsi, non seulement l'Agence eSanté et les professionnels de santé peuvent, en fonction du traitement en cause, être considérés comme responsables du traitement des données contenues dans le DSP, mais aussi d'autres entités comme celles mentionnées ci-dessus.

La CNPD ne peut que soutenir l'approche des auteurs des amendements de préciser dans le corps du texte les obligations respectives des différentes responsables du traitement comme exigé par l'article 26 du RGPD.

[268] Arrêt du 29 juillet 2019, Fashion ID GmbG & Co. KG / Verbraucherzentrale NRW eV, C-40/17, EU:C:2018:1039, point 70; voir, en ce sens, arrêt du 10 juillet 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, point 66.

Néanmoins, comme on est clairement en présence d'une responsabilité conjointe et non pas d'une responsabilité unique de l'Agence eSanté, la CNPD estime nécessaire de modifier l'article 60*ter* (4) du Code de la sécurité sociale afin de prévoir les responsabilités des différents intervenants.

II. Ad Amendement 2

L'article 2 paragraphe (2) du projet de règlement grand-ducal mentionne toujours que le patient non affilié bénéficiant de soins de santé par un prestataire de soins établi au Luxembourg peut demander l'ouverture d'un DSP moyennant un formulaire de demande à adresser à l'Agence eSanté. Le commentaire des articles de la version initiale du projet de règlement grand-ducal précisait à cet égard que ledit formulaire doit être accompagné des *« pièces justificatives nécessaires »*. Or, au vu du principe de proportionnalité et de nécessité (principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre c) du RGPD), la CNPD a considéré dans son avis du 5 avril 2018 que cette définition manque de clarté et de précision et elle a estimé nécessaire d'énumérer de manière plus précise et concise ces *« pièces justificatives nécessaires »* dans le corps du texte. Or, les auteurs des amendements n'ont pas tenu compte de cette remarque de la Commission nationale.

Par ailleurs, même si l'article 2, paragraphe (3), lettre f) nouveau précise dorénavant que le patient est également informé par l'Agence eSanté du contenu de son DSP au moment de son activation, la Commission nationale se demande toujours quel est ce contenu, c'est-à-dire quelles sont les catégories de données qui sont contenues dans le DSP lors de son activation. Comme dans son avis du 5 avril 2018, elle se pose toujours la question si les données issues des annuaires référentiels d'identification des patients et des prestataires de soins seront aussi intégrées dans les DSP et dans l'affirmative, elle estime que ces catégories de données devraient être ajoutées à celles déjà prévues à l'annexe 1 du projet de règlement grand-ducal sous le numéro (2).

III. Ad Amendement 4

L'amendement 4 vise à modifier l'article 4 du projet de règlement grand-ducal concernant la fermeture et la suppression du DSP. De manière générale, la CNPD renvoie à ses commentaires formulés dans son avis du 5 avril 2019 concernant la durée de conservation des données suite à la fermeture du DSP, dans lequel elle a considéré qu'une durée d'archivage intermédiaire des données de dix ans apparaît comme excédant celle nécessaire au regard des finalités d'exercice du droit d'accès et d'une éventuelle réouverture du DSP et qu'une durée de conservation des données de cinq ans suite à une fermeture d'un DSP serait plus appropriée et respecterait le principe de la limitation de conservation prévu par l'article 5 paragraphe (1) lettre e) du RGPD.

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

même doit être détruit intégralement, comme le prévoit d'ailleurs l'article R1111-34 du Code de la santé publique français.

De même, la CNPD estime qu'il est primordial qu'en cas de clôture d'un DSP, son titulaire soit informé que les données qu'il contient ne seront plus accessibles, d'autant plus que le DSP peut contenir ses volontés en matière de don d'organes, des directives anticipées ou une information relative à des dispositions de fin de vie selon l'article 6 paragraphe (2) lettre b) du projet de règlement grand-ducal.

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

IV. Ad amendement 5

Le commentaire de l'amendement 5, visant à modifier l'article 5 du projet de règlement grand-ducal concernant l'accès au DSP par les professionnels de santé, précise qu' *« il y a lieu de bien marquer les deux étapes : activation de son compte par le titulaire du dossier de soins partagé et activation de son compte par le professionnel de santé. »* Or, malgré les modifications proposées par l'amendement, il ne ressort toujours pas du projet de règlement grand-ducal si l'activation de son compte sur la plateforme moyennant ses identifiants personnels et la connexion ultérieure est facultative pour les professionnels de santé. Pour cette hypothèse, la CNPD avait déjà constaté dans son avis du 5 avril 2018 qu'il y aurait donc un système « d'opt-out » pour les patients, tandis que pour les professionnels de santé un système « d'opt-in » s'appliquerait.

Finalement, des explications claires des auteurs des amendements sur les acteurs visés par la notion de « collectivité de santé » font encore défaut dans le corps du texte. Dans son avis du 23 octobre 2018, le Conseil d'État a également demandé aux auteurs de préciser les entités visées par la notion de « collectivité de santé ».

V. Ad Amendement 6

Par l'amendement 6, modifiant l'article 6 du projet de règlement grand-ducal encadrant les droits d'accès et d'écriture du titulaire, les auteurs ont pris en compte l'importance de l'autodétermination informationnelle du patient en supprimant dans le texte que la modification des droits d'accès ne s'applique pas au médecin référent et aux professionnels d'un service d'urgence d'un établissement hospitalier. En effet, le nouveau texte permet au titulaire d'interdire l'accès à son dossier intégral à des professionnels de santé qu'il désigne expressément ou de rendre certaines données inaccessibles à certains professionnels de santé, sans exception. Comme le précise le commentaire de l'amendement respectif, *« cette modification tient compte de la remarque du Conseil d'État qui soulève que la liste limitative de droits d'opposition est contraire à l'article 60quater, paragraphe 4 du Code de la*

sécurité sociale qui accorde un droit général au titulaire de pouvoir s'opposer à tout moment au partage de données le concernant. »

Par ailleurs, la CNPD félicite les auteurs des amendements d'avoir ajouté à l'article 6 paragraphe (3) alinéa 4 du projet de règlement grand-ducal la possibilité pour le titulaire de demander l'effacement de ses données personnelles auprès du professionnel de santé ou de l'Agence eSanté. Or, similairement à ce que la CNPD avait constaté dans son avis du 5 avril 2018 dans le cadre de la possibilité pour le titulaire de rendre inaccessible certaines données spécifiques à un ou plusieurs professionnels de santé, la CNPD estime que la possibilité de demander l'effacement de données personnelles ne correspond pas à la réalité du système tel qu'il est conçu. Elle se demande notamment comment concrètement l'Agence eSanté ou les professionnels de santé entendent faire droit à des requêtes d'effacement de données personnelles spécifiques. En effet, le DSP ne contient que peu de données individuelles ou structurées, mais se compose en réalité et surtout de documents scannés, chaque document contenant une multitude d'informations ou de données de santé relatives à un patient.

La CNPD réitère donc son soucis de savoir comment il pourra être garanti qu'un titulaire puisse demander l'effacement de ses données personnelles (par exemple des données relatives à une interruption volontaire de grossesse) contenues dans plusieurs documents médicaux scannés. A moins de supprimer l'intégralité des documents, elle est d'avis qu'il ne sera pratiquement pas possible d'effacer certaines données spécifiques dans l'ensemble des documents contenant ces données spécifiques.

VI. Ad Amendement 8

Tout d'abord, la CNPD renvoie à son avis du 5 avril 2018, dans lequel elle avait déjà critiqué qu'une matrice des accès par défaut, comme celle prévue à l'annexe 1 du projet sous examen, doive par principe être considérée comme étant contraire au principe du « Privacy by Design » prévu par l'article 25 paragraphe (2) du RGPD.

Par ailleurs, l'article 7 nouveau paragraphe (1) alinéa 2 du projet de règlement grand-ducal prévoit des modalités spécifiques pour le *« classement d'un type de donnée au sein d'une catégorie de données »*. Étant donné que dans le DSP figurent surtout des documents scannés qui ne présentent aucune granularité, la CNPD rappelle que le texte du projet ne correspond pas à la réalité de la configuration des systèmes mis en place. Elle se demande notamment comment l'Agence eSanté en tant que responsable du traitement va maîtriser la situation dans laquelle plusieurs catégories de données se retrouvent dans un même document scanné et qu'un professionnel de santé n'a droit d'accéder uniquement à une catégorie, mais non pas à une autre ?

De même, la CNPD a déjà eu l'occasion de souligner[269] que la liste des destinataires ne devrait pas à l'avenir être élargie à d'autres catégories de personnes (comme notamment des compagnies d'assurances privées, des employeurs, des praticiens de la médecine agissant en tant qu'expert pour le compte de tiers, etc.) et elle avait

[269] Voir la délibération n°345/2010 du 24 novembre 2010 relatif au projet de loi n°6196 portant réforme du système de soins de santé, ainsi que la délibération n°242/2018 du 5 avril 2018 sur le projet de règlement grand-ducal sous examen.

proposé aux auteurs d'ajouter une disposition dans ce sens dans le corps du texte du projet de règlement grand-ducal sous avis. Or, les auteurs des amendements n'ont pas tenu compte de cette recommandation.

En ce qui concerne le droit à l'information des personnes concernées, la CNPD note avec satisfaction que le paragraphe (3) nouveau de l'article 7 du projet de règlement grand-ducal impose dorénavant aux professionnels de santé l'obligation de fournir aux titulaires au moment de la collecte de leurs données, les informations visées à l'article 13, paragraphes 1 et 2 du RGPD. Néanmoins, la CNPD tient à insister que cette obligation d'informer les titulaires d'un DSP s'impose aussi à une collectivité de santé (par exemple un laboratoire, un centre d'aide et de soins, etc.). Il est primordial que le patient comprenne qu'une collectivité de santé, voire un professionnel de santé exerçant à titre individuel, entend accéder à son DSP et qu'il a la possibilité de refuser cet accès.

Finalement, pour répondre aux exigences légales du RGPD, un professionnel de santé, exerçant à titre individuel ou dans une collectivité de santé, devra être en mesure de démontrer que cette information au patient a bien eu lieu. La CNPD rappelle dans ce contexte sa recommandation déjà formulée en 2010 que le recours à une « carte de santé » de type « carte vitale française » ou « elektronische Gesundheitskarte » allemande faciliterait ce procédé, de même qu'une telle carte faciliterait l'utilisation d'autres procédés / fonctionnalités dans le cadre du système du DSP (tel que par exemple le recours à un identifiant de connexion peu pratique ou convivial).

VII. <u>Ad amendement 10</u>

Déjà dans son avis du 5 avril 2018, la CNPD a estimé que sur base des principes de minimisation des données et de la limitation de la conservation (article 5 paragraphe (1) lettres c) et e) du RGPD) et en considérant que le DSP a comme finalité principale le partage et l'échange de données utiles et pertinentes entre professionnels de santé pour une meilleure qualité de soins, que le DSP n'a pas comme vocation d'être exhaustif, qu'il ne se substitue pas aux dossiers tenus par les professionnels de santé ou les établissements hospitaliers et qu'il n'a certainement pas une finalité de stockage ou d'archivage de données, qu'une durée de conservation de cinq ans à compter du versement des données dans le DSP est suffisante et appropriée au regard des finalités réellement et légalement poursuivies.

Le Conseil d'État avait formulé des réserves similaires dans son avis du 23 octobre 2018 en estimant que la disposition concernant la durée de conservation générale de 10 ans *« manque de flexibilité et que le professionnel de santé qui introduit une donnée devrait pouvoir déterminer la durée de conservation de la donnée en fonction de son utilité et de sa pertinence, et partant, fixer la date de son effacement en concertation avec le titulaire, date qui pourra, le cas échéant, être modifiée par la suite selon l'évolution de l'état de santé du titulaire. »*

La CNPD note que même si la durée de conservation générale de 10 ans a été maintenue, par l'introduction du paragraphe (5) alinéa 2 de l'article 9 nouveau, le professionnel de santé peut, avec l'accord du titulaire, déroger à ce délai et déterminer une durée de conservation plus courte en fonction de l'utilité et de la pertinence de la donnée

pour l'état de santé du titulaire. Par ailleurs, la CNPD félicite les auteurs des amendements d'avoir prévu à alinéa 3 dudit paragraphe que le professionnel de santé peut, avec l'accord du titulaire, déterminer que certaines données médicales jugées utiles et pertinentes à vie pour l'état de santé du titulaire, sont conservées jusqu'à la fermeture du dossier de soins partagé. Par ailleurs, il est précisé que *« l'accord du titulaire est daté et consigné dans son espace d'expression personnelle dans l'application dossier de soins partagé. »*

VIII. Ad amendement 11

L'amendement 11 vise à modifier l'article 10 du projet de règlement grand-ducal concernant la sécurité de la plateforme.

Dans son avis du 5 avril 2018, la CNPD avait critiqué qu'en ce qui concerne particulièrement les éditeurs d'un programme informatique connecté à la plateforme nationale, on pourrait interpréter l'ancien article 11 paragraphe (2) du projet de telle manière que ces derniers pourraient se connecter directement à la plateforme. Or, la CNPD avait souligné qu'il n'est pas acceptable que des acteurs IT aient eux-mêmes un accès direct au DSP, ceci n'étant absolument pas la pratique en la matière.

La CNPD prend note que par l'amendement 11, le terme précité de l'« éditeur d'un programme informatique » est remplacé par le terme « sous-traitant » dans le paragraphe 2, alinéa 1 et 3, et les auteurs expliquent dans le commentaire *« qu'il est admis que les prestataires aient besoin dans l'exécution des missions leur attribuées dans le cadre de l'application dossier de soins partagés, pour des raisons techniques et organisationnelles, de sous-traitants leur mettant en place des mesures de sécurité pour garantir la disponibilité, l'authenticité, l'intégrité, la confidentialité et la traçabilité des données échangées sur la plateforme. »*

La CNPD tient à réitérer dans ce contexte ses réserves concernant l'accès aux DSP par des acteurs autres que les professionnels de santé. Le projet actuel ne fournit à cet égard aucun encadrement législatif qui irait au-delà des principes généraux prévus au RGPD, notamment en matière de sous-traitance (article 28 du RGPD). Or, un accès à une grande partie des données de santé de la population quasi-entière justifierait et rendrait nécessaire une telle précision. A titre d'exemple, la CNPD se réfère aux mesures législatives qui ont été prises au niveau du secteur bancaire pour encadrer et protéger l'accès aux données financières. Selon l'avis de la CNPD, les données de santé, spécifiquement réglementées par l'article 9 du RGPD, sont d'une sensibilité supérieure aux données financières – et devraient de ce fait faire l'objet d'une protection tout au moins équivalente. Sans vouloir être exhaustif, la CNPD attire aussi l'attention sur le fait que dans d'autres États-membres des mécanismes d'accréditation permettent d'assurer à ce que l'accès à de telles données soit soumis à un contrôle indépendant ou tout au moins sous le contrôle de l'État.

La CNPD rappelle que sans encadrement supplémentaire chaque prestataire de santé peut recourir à des sous-traitants sur base de sa propre évaluation de risque – tout en exposant potentiellement l'intégralité des données

contenues au DSP. La situation actuelle, se manifestant par une absence de pouvoir de l'Agence eSanté de contrôler qui a accès au système du DSP, rendrait donc quasiment impossible tout pouvoir de ladite Agence d'assurer un niveau élevé de sécurité du système.

Finalement, la Commission nationale constate qu'une grande partie de ses recommandations ou questions concernant l'actuel article 10 sur la sécurité de la plateforme n'ont pas été prises en compte par les auteurs des amendements.

Ainsi, la Commission nationale tient à rappeler certaines de ses observations formulées dans son avis précité concernant l'ancien article 11 intitulé : « Sécurité de la plateforme électronique nationale » :

« Selon l'article 11 paragraphe (1) du projet, l'Agence eSanté s'engage à mettre en œuvre un système de management de la sécurité de l'information certifié conforme à la Norme internationale ISO/IEC 27001. Néanmoins, la CNPD suggère de préciser dans le texte du projet de règlement grand-ducal le périmètre minimum sur lequel ladite certification ISO devra se porter. Le périmètre devra porter sur l'intégralité des systèmes, processus et éléments organisationnels impliqués directement ou indirectement sur la plateforme et reflétant bien, le cas échéant, la situation de la responsabilité conjointe.

L'article 11 paragraphe (1) lettre e) du projet envisage la « mise en place d'audits de sécurité annuels ». L'article 32 paragraphe (1) du RGPD contient dans ce contexte une liste non exhaustive de mesures techniques et organisationnelles que le responsable du traitement et le sous-traitant doivent mettre en œuvre afin de garantir un niveau de sécurité adapté au risque. Une de ces mesures est précisément la mise en place d'une « procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement » (article 32 paragraphe (1) lettre d) du RGPD). Si les auteurs du projet de règlement grand-ducal sous avis entendent viser cette disposition du RGPD, ils devraient en préciser les détails dans le corps du texte. Entre autres, la CNPD estime nécessaire de définir si ces audits seront effectués par des auditeurs indépendants ou par des auditeurs externes à l'Agence eSanté. De même, le projet reste muet sur le périmètre spécifique de ces audits, alors qu'une approche régulièrement adoptée en la matière se manifeste par un plan d'audit tri-annuel validé par le conseil d'administration pour qu'au bout de 3 ans, toutes les procédures ont été auditées.

Le paragraphe (2) dudit article oblige les prestataires et éditeurs d'un programme informatique connecté à la plateforme nationale à mettre en œuvre des mesures de sécurité appropriées au regard de son type, de sa taille, de ses processus ou de ses activités. Or, la CNPD est d'avis que la taille du prestataire ou éditeur n'est pas à considérer comme un critère pertinent dans ce contexte. En effet, l'article 32 paragraphe (1) du RGPD précise que les mesures techniques et organisationnelles à mettre en place doivent être adaptées à « l'état des connaissances, des coûts de mise en oeuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des

risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques […]. »
Le risque peut par exemple être particulièrement élevé si un prestataire a accès à un grand nombre de DSP.

[…]

Enfin, la Commission nationale se demande à quelles intervalles l'Agence eSanté entend mettre en œuvre les mesures de sensibilisation du personnel telles que prévues à l'article 11 paragraphe (2) lettre e) du projet. »

IX. Ad amendement 12

L'amendement 12 vise à modifier certains termes de l'ancien article 12 intitulé « Modalités techniques de versement des données au dossier de soins partagé et interopérabilité » du projet de règlement grand-ducal qui devient le nouvel article 11 du projet de règlement grand-ducal.

La Commission nationale constate dans ce contexte qu'aucune de ses remarques n'a été considérée par les auteurs des amendements.

Ainsi, la Commission nationale tient à réitérer ses observations formulées dans son avis précité concernant l'ancien article 12 intitulé « Modalités techniques de versement des données au dossier de soins partagé et interopérabilité » :

« Selon l'article 12 paragraphe (2) alinéa 4 lettre a) du projet, les tests mentionnés au paragraphe 2, alinéa 3 lettre a) dudit article seront effectués non pas par l'Agence eSanté, mais par un organisme ou une société experte en interopérabilité des systèmes de santé. La CNPD se pose surtout la question qui devra assumer les frais concernant les travaux de cet expert, et surtout qui désignera cet expert et sur base de quels critères les compétences de ce dernier seront vérifiées ?

Le paragraphe (2) de l'article 12 du projet continue en ce sens qu'une attestation de conformité sera délivrée par l'Agence eSanté sur base du résultat des tests réalisés par l'expert susmentionné. Or, sur quels critères l'Agence eSanté va-t-elle baser sa décision et comment va-t-elle se décider concrètement ? Est-ce que des représentants ne faisant pas partie de l'Agence eSanté seront impliqués pour garantir l'indépendance de la décision? La CNPD recommande ainsi aux auteurs d'indiquer dans le projet que l'Agence eSanté doit mettre en place un règlement d'ordre intérieur fixant les procédures de délivrance, de blocage et de retrait des attestations afin de garantir une équité de traitement des attestations pour tous les acteurs.

Enfin, dans l'article 12 paragraphe (2) alinéa 6 du projet il est indiqué que l'attestation des résultats des tests reste valable tant qu'aucune modification ne l'affecterait. Or cette approche ne correspond pas au bonnes

pratiques en la matière, car même sans changement dans les systèmes, de nouvelles vulnérabilités dans des applications existantes pourraient tout à fait être découvertes et par la suite potentiellement exploitées. Ainsi la CNPD estime qu'une « procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement » telle que préconisée dans l'article 32 (1) (d) du RGPD devrait être mise en place – et ceci indépendamment si des modifications ont eu lieu. »

Ainsi décidé à Esch-sur-Alzette en date du 18 octobre 2019.

La Commission nationale pour la protection des données

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

ANNEXES

5

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7462 portant modification de la loi modifiée du 5 juin 2009 relative à la qualification initiale et à la formation continue des conducteurs de certains véhicules routiers affectés aux transports de marchandises ou de voyageurs et modifiant la loi modifiée du 27 juillet 1993 ayant pour objet 1. le développement et la diversification économiques et 2. l'amélioration de la structure générale et de l'équilibre régional de l'économie.

Délibération n°52/2019 du 15 novembre 2019

Conformément à l'article 57, paragraphe 1er, lettre (c) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

Par courrier en date du 20 juin 2019, Monsieur le Ministre de la Mobilité et des Travaux publics a invité la Commission nationale à se prononcer sur le projet n°7462 portant modification de la loi modifiée du 5 juin 2009 relative à la qualification initiale et à la formation continue des conducteurs de certains véhicules routiers affectés aux transports de marchandises ou de voyageurs et modifiant la loi modifiée du 27 juillet 1993 ayant pour objet 1. le développement et la diversification économiques et 2. l'amélioration de la structure générale et de l'équilibre régional de l'économie (ci-après le « projet de loi »).

Le présent projet de loi a pour objet de transposer en droit national la directive (UE) 2018/645 du Parlement européen et du Conseil du 18 avril 2018 modifiant la directive 2003/59/CE relative à la qualification initiale et à la formation continue des conducteurs de certains véhicules routiers affectés aux transports de marchandises ou de voyageurs ainsi que la directive 2006/126/CE relative au permis de conduire (ci-après la « directive »). Cette transposition en droit national intervient en modifiant la loi modifiée du 5 juin 2009 relative à la qualification initiale et à la formation continue des conducteurs de certains véhicules routiers affectés aux transports de marchandises ou de voyageurs et modifiant la loi modifiée du 27 juillet 1993 ayant pour objet 1. le développement et la diversification économiques et 2. l'amélioration de la structure générale et de l'équilibre régional de l'économie (ci-après la « loi modifiée du 5 juin 2009 »), ainsi que par une modification du règlement grand-ducal du 2 octobre 2009 relatif aux matières enseignées dans le cadre de la qualification initiale et de la formation continue des

conducteurs de certains véhicules routiers affectés aux transports de marchandises ou de voyageurs ainsi qu'aux critères d'agrément pour dispenser cet enseignement.

L'une des nouveautés de la directive est la mise en place entre les États-membres d'un réseau électronique dont le but est de permettre l'échange, entre les États-membres, d'informations sur les certificats de formation délivrés ou retirés aux conducteurs de certains véhicules routiers. Ce réseau est visé à l'article 6 de la directive qui introduit un nouvel article 10 bis intitulé *« Réseau d'exécution »* dans la directive 2003/59/CE relative à la qualification initiale et à la formation continue des conducteurs de certains véhicules routiers affectés aux transports de marchandises ou de voyageurs (ci-après la « directive 2003/59/CE). Le considérant 10 de la directive précise à ce titre que *« Les États-membres, en coopération avec la Commission, devraient échanger par voie électronique des informations relatives aux certificats d'aptitude professionnelle (CAP). Ils devraient développer la plateforme électronique nécessaire, en tenant compte pour ce faire d'une analyse coûts-avantages réalisée par la Commission, en envisageant notamment la possibilité d'étendre le réseau des permis de conduire de l'Union européenne mis en place au titre de la directive 2006/126/CE. Cela permettra entre autres aux États-membres d'accéder facilement aux informations relatives aux formations accomplies, qui ne figurent pas sur le permis de conduire du conducteur. »*[270] .

De manière générale, le présent avis ne portera pas sur le cadre légal de la directive, qui a été décidé par le législateur européen lui-même, mais se limitera à des observations concernant des dispositions où les auteurs du projet de loi ont usé de leur marge de manœuvre laissée aux États-membres lors de la transposition en droit national d'une directive européenne. En effet, une telle directive n'instaure qu'une obligation de résultat, tout en laissant les États-membres de l'Union européenne libres quant aux formes et moyens à prendre pour y parvenir[271].

Le présent avis se limitera donc à commenter les nouvelles dispositions introduites par la directive concernant la mise en place d'un réseau électronique entre les États-membres, tel que décrit ci-avant. Ces dispositions sont transposées en droit national à l'article 4 du projet de loi qui insère un nouvel article 6 bis intitulé *« Banque de données électronique et échanges de données »* dans la loi modifiée du 5 juin 2009.

1. Sur la banque de données électronique visée par le nouvel article 6 bis de la loi modifiée du 5 juin 2009

i. Remarques préliminaires

Tout d'abord, il y a lieu de relever qu'il ressort des commentaires des auteurs du projet de loi relatifs au nouvel article 6 bis introduit par la loi sous avis que *« les données relatives aux permis de conduire au Luxembourg se trouvent dans une banque de données dont le propriétaire est le ministère ayant les Transports dans ses attributions (…) », les auteurs précisent encore que « les informations relatives à la formation professionnelle (catégorie, durée de validité) se trouvent actuellement déjà dans cette banque de données nationale ».*

[270] Le « réseau des permis de conduire de l'Union européenne mis en place au titre de la directive 2006/126/CE » précité découle de l'article 15 de la directive 2006/126/CE et est actuellement en place au sein de l'Union européenne. Ce réseau s'intitule le système « RESeau PERmis de conduire ». Ce système fonctionne d'ailleurs en concurrence avec un autre système appelé le système European Car and Driving Licence Information System. Ces deux systèmes permettent notamment l'échange de données relatifs aux permis de conduire dans les pays de l'Union européenne.

[271] L'article 288 du traité sur le fonctionnement de l'Union européenne dispose que la « La directive lie tout État-membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens. »

En vertu de ce qui précède, la Commission nationale se demande alors si la banque de données électronique, prévue au nouvel article 6 bis introduit par la loi sous avis, est intégrée dans le fichier préexistant relatif aux permis de conduire, c'est-à-dire la *« base de données nationale »*, ou s'il s'agit de créer un fichier distinct de la *« base de données nationale »* préexistante précitée ? De plus, la CNPD s'interroge encore sur l'articulation en pratique entre les différents traitements de données mis en œuvre à travers cette *« base de données nationale »* et / ou la *« banque de données électronique »* visée par le projet de loi sous avis ?

En tout état de cause, la Commission nationale se félicite que, du point de vue de la sécurité juridique, soit prévu, au paragraphe (1) du nouvel article 6 bis introduit par la loi sous avis, le principe de la création d'une *« banque de données électronique reprenant les informations relatives aux certificats de formations délivrés ou retirés prévus à l'article 3 [de la loi modifiée du 5 juin 2009] »*. D'après le paragraphe (3) dudit article, le ministre ayant dans ses compétences la loi sous avis (ci-après le « ministre ») en est le responsable du traitement et le Centre des technologies de l'information de l'État (ci-après le « CTIE »), la Société Nationale de Circulation Automobile (ci-après la « SNCA ») et les organismes de formation prévus à l'article 6 de la loi modifiée du 5 juin 2009 (qui peuvent être des organismes privés ou publics) ont la qualité de sous-traitant. De plus, le paragraphe (2) dudit article énumère les finalités des traitements mis en œuvre dans le cadre de la loi sous avis et le paragraphe (4) du nouvel article 6 bis précise encore les données transmises par les organismes de formation au ministre.

La CNPD salue que le principe de la création d'une telle banque de données ou d'un tel traitement de données ainsi que les précisions précitées soient prévues par le projet de loi. Ces dispositions légales établissent ainsi, conformément à l'article 6, paragraphe (3) du RGPD, les spécifications de ce nouveau traitement dont sera investi le ministre.

En effet, il convient de rappeler que la tenue d'un fichier de données à caractère personnel collectées et traitées par une autorité administrative doit reposer sur une base légale conformément à l'article précité, lu ensemble avec son paragraphe (1) lettres c) et e)[272], qui dispose que : *« Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par :*

a. le droit de l'Union; ou

b. le droit de l'État-membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice 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

[272] L'article 6, paragraphe (1), lettres c) et e) dispose que : *« Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : (…) c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; (…) e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; (…) ».*

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. »

Il résulte de ce qui précède que cet article prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans ces deux cas de figure, le fondement et les finalités des traitements de données doivent spécifiquement être définis soit par le droit de l'Union européenne, soit par le droit de l'État-membre auquel le responsable du traitement est soumis.

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

En vertu des dispositions précitées, ces bases légales devraient établir des dispositions spécifiques visant à déterminer, entre autres, les types de données traitées, les personnes concernées, les entités auxquelles les données peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

Ainsi, au vu des développements qui précèdent, et bien que le principe d'un nouveau traitement de données via la création de la *« banque de données électronique »,* tel que visé au paragraphe (1) du nouvel article 6 bis de la loi modifiée du 5 juin 2009, soit prévu, la Commission nationale relève toutefois que certains éléments spécifiques relatifs au traitement de données ne sont pas (ou pas suffisamment) précisés dans la loi sous avis.

ii. <u>Sur le rôle des différents acteurs</u>

Comme indiqué précédemment, la Commission nationale se félicite de ce que le paragraphe (3) du nouvel article 6 bis de la loi modifiée du 5 juin 2009, introduit par la loi sous avis, précise le rôle des différents acteurs dans le cadre des traitements de données à caractère personnel visés par l'article précité.

La CNPD salue que les auteurs du projet de loi aient précisé que le ministre a la qualité de responsable du traitement conformément aux dispositions 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. Néanmoins,

la notion de responsable du traitement n'est pas définie dans la loi précitée mais est définie à l'article 4, point 7) du RGPD[273]. Dans ce contexte, la Commission nationale estime plus judicieux de se référer directement aux dispositions légales du RGPD.

Par ailleurs, concernant le CTIE, la SNCA et les organismes de formation agréés visés à l'article 6 de la loi modifiée du 5 juin 2009, la Commission nationale comprend qu'ils agissent en tant que sous-traitant du ministre au sens du RGPD. Dans un souci de clarté, le renvoi à la définition de « sous-traitant », visée à l'article 4, point 8) du RGPD[274] pourrait être mentionnée à la fin du deuxième alinéa du paragraphe (3) du nouvel article 6 bis. Concernant le rôle du sous-traitant, il y a lieu de rappeler que conformément à l'article 28 du RGPD, celui-ci *« ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement »*.

En outre, il conviendrait de préciser si la SNCA, dans le cadre de la loi sous avis, agit en tant que sous-traitant du ministre dans le cadre de ses missions légales telles que prévues à l'alinéa 1er du paragraphe (4) de l'article 2 de la loi du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques (telle qu'elle a été modifiée), qui dispose que : *« Le ministre peut confier à la Société Nationale de Circulation Automobile, en abrégé SNCA, des tâches administratives relevant de la gestion des permis de conduire »*.

iii. <u>Sur les finalités du traitement de données à caractère personnel</u>

La Commission nationale se félicite du fait que les finalités spécifiques du traitement soient déterminées et listées au paragraphe (2) du nouvel article 6 bis de la loi modifiée du 5 juin 2009.

Tout d'abord, il convient de relever que seules les dispositions légales visées aux points 1), 3) et 4) du paragraphe (2) de l'article précité ont pour objet de transposer le nouvel article 10 bis de la directive 2003/59/CE, introduit par la directive.

En ce qui concerne la finalité visée au point 3) du paragraphe (2) dudit article[275], la Commission nationale se demande si le terme *« interconnexion »* ne pourrait pas être remplacé par le terme *« échange »*, dans la mesure où le nouvel article 10 bis de la directive 2003/59/CE, introduit par la directive, n'emploie pas ce terme et mentionne la notion d' *« échange »*. En effet, en matière de protection des données le concept d' *« interconnexion »*[276] signifie que les traitements des données sont reliés et peuvent être gérés par les responsables des différents traitements concernés. Dans la mesure où les auteurs de la loi sous avis semblent vouloir viser un système de transmission de données par voie électronique et non une réelle interconnexion, il conviendrait dès lors, afin d'éviter toute confusion, d'en adapter la terminologie comme suggéré ci-avant.

Concernant la finalité visée au point 4) du paragraphe (2) du nouvel article 6 bis, la Commission nationale se demande, au vu des développements qui précèdent, si cette finalité ne pourrait pas être regroupée avec la finalité

[273] L'article 4, point 7) du RGPD définit le responsable du traitement comme : *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État-membre,, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État-membre, »*.

[274] L'article 4, point 8 du RGPD définit le sous-traitant comme : *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »*.

[275] La finalité mentionnée au point 3), paragraphe (2) du nouvel article 6 bis de la loi modifiée du 5 juin 2009 vise *« l'interconnexion avec les réseaux électroniques nationaux des autres États-membres de l'Union européenne telle que prévue à l'article 10 bis de la directive 2003/59/CE »*.

[276] La version initiale de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, désormais abrogée, définissait à l'article 2, lettre (j) l'interconnexion comme : *« toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou d'autres responsables du traitement »*.

visée au point 3) du paragraphe (2) du nouvel article 6 bis dans un seul point, alors que ces deux paragraphes semblent avoir la même finalité, à savoir l'échange d'informations relatives aux formations.

En effet, la finalité visée au point 4) du paragraphe (2) du nouvel article 6 bis est l' *« échange d'informations relatif aux certificats de formation prévus à l'article 3 »* et la finalité visée au point 3) du même article se réfère à la finalité mentionnée dans le nouvel article 10 bis de la directive 2003/59/CE, introduit par la directive, qui vise l'échange d'informations *« sur les CAP délivrés ou retirés »*.

iv. Sur les catégories de données à caractère personnel et les personnes concernées

La Commission nationale se félicite de ce que les catégories de données à caractère personnel collectées et transmises par les organismes de formation agréés au ministre soient spécifiées et énumérées avec autant de précision au nouvel article 6 bis paragraphe (4) de la loi modifiée du 5 juin 2009, introduit par la loi sous avis.

Toutefois, la CNPD se demande quelles sont les catégories de données visées par le terme *« informations nécessaires au financement de la formation »*, employé à la lettre c), paragraphe (4) de l'article précité, alors qu'aucune précision supplémentaire concernant ce type de données n'est apportée dans les commentaires des auteurs du projet de loi concernant ces dispositions.

De plus, la Commission nationale s'interroge également sur la collecte ou non de certaines catégories de données qui sont visées par les auteurs du projet de la loi sous avis, dans leurs commentaires relatifs au nouvel article 6 bis, sans toutefois être reprises dans le texte dudit article. Il convient, en effet, de constater que les *« informations relatives à la formation professionnelle (catégorie, durée de validité) »* et les *« informations sur des procédures administratives relatives aux certificats »*, bien que mentionnées dans les commentaires du projet de loi, n'apparaissent pas dans le texte du nouvel article 6 bis.

v. Sur l'accès aux données à caractère personnel

Il convient de relever que les dispositions énoncées au paragraphe (6) du nouvel article 6 bis de la loi modifiée du 5 juin 2009, introduit par la loi sous avis, prévoient un accès *« aux données contenues dans la banque de données »* pour les membres de la Police grand-ducale et les agents de l'administration des douanes et accises dans le cadre de la finalité visée par le paragraphe (2), point 1) de l'article précité.

La Commission nationale comprend que ces nouvelles dispositions légales visent à mettre en œuvre les dispositions du paragraphe (3) du nouvel article 10 bis de la directive 2003/59/CE, introduit par la directive, qui dispose que : *« Les États-membres veillent à ce que les données à caractère personnel soient traitées aux seuls fins de contrôler*

le respect de la présente directive, et en particulier des exigences de formation établies dans la présente directive, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil ».

Or, dans la mesure où une loi doit être suffisamment claire et précise afin de permettre aux personnes concernées de connaître l'étendue des limitations, ainsi que les conséquences éventuelles pour elles[277], il conviendrait de préciser le cadre légal des contrôles pouvant être effectués par les membres de la Police grand-ducale et les agents de l'administration des douanes et accises. La Commission nationale recommande, dès lors, d'insérer à la fin du paragraphe (6) du nouvel article 6 bis, la formulation suivante : *« conformément à leurs pouvoirs de contrôle tels que visés au paragraphe (3) de l'article 7 de la présente loi »*[278].

Par ailleurs, l'accès prévu aux membres de la Police grand-ducale au titre de la loi sous avis ne serait-il pas déjà prévu par les points 7) et 8) de l'article 43 de la loi du 18 juillet 2018 sur la Police grand-ducale qui prévoit que : *« Dans l'exercice de leurs missions de police judiciaire et de police administrative, les membres de la Police ayant la qualité d'officier de police judiciaire ou d'officier de police administrative ont accès direct, par un système information, aux traitements de données à caractère personnel suivant : […] 7° le fichier des titulaires et demandeurs de permis de conduire exploité pour le compte du ministre ayant le Transport dans ses attributions ; 8° le fichier des véhicules routiers et de leurs propriétaires et détenteurs, exploité pour le compte du ministre ayant les Transports dans ses attributions […] »* ?

vi. <u>Sur la traçabilité des accès</u>

Conformément à l'article 5 paragraphe (1), lettre f) du RGPD les données à caractère personnel doivent être *« traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ».*

En outre, l'article 32 du RGPD dispose que : *« le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».* Pareilles mesures doivent être mises en œuvre afin d'éviter notamment des accès non-autorisés aux données ou des fuites de données.

Parmi ces mesures de sécurité, la Commission nationale estime important que seules les personnes qui en ont besoin dans l'exercice de leurs fonctions et de leurs tâches professionnelles soient habilitées à avoir accès aux données nécessaires. Dans ce contexte, il est vivement recommandé de définir une politique de gestion des accès, afin de pouvoir identifier dès le début la personne ou le service, au sein de chaque entité ou administration concernée, qui aurait accès aux données ou, dans le cadre des administrations, à l'interface informatique mise à disposition par le CTIE, et à quelles données précises cette personne ou ce service aurait accès.

[277] Voir entre autres CourEDH, Zakharov c. Russie [GC], n°47413/06, § 228-229, 4 décembre 2015.

[278] Article 7, paragraphe (3) de la loi modifiée du 5 juin 2009 dispose que : *« Les membres de la police grand-ducale ainsi que les agents de l'Administration des douanes et accises agissant dans le cadre des contrôles de véhicules effectués dans l'exercice des fonctions qui leur sont conférées par la législation sur les transports routiers et la circulation routière sont chargés de contrôler l'exécution des dispositions de la présente loi et de ses règlements d'exécution et de dresser procès-verbal des infractions ».*

En outre, il est nécessaire de prévoir un système de journalisation des accès. Enfin, la CNPD recommande que les données de journalisation soient conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.

2. Sur l'échange de données à caractère personnel

Le paragraphe (5) du nouvel article 6 bis de la loi modifiée du 5 juin 2009 vise à transposer le paragraphe (1) du nouvel article 10 bis de la directive 2003/56/CE, introduit par la directive.

Tout d'abord concernant l'échange de données à caractère personnel, la Commission nationale tient à rappeler que les données à caractère personnel peuvent circuler librement depuis le Grand-Duché de Luxembourg au sein de l'Espace économique européen, tant que les principes généraux du RGPD sont respectés.

Par ailleurs, la Commission nationale se demande si la formulation du paragraphe (5) du nouvel article 6 bis de la modifiée du 5 juin 2009 n'aurait pas une portée plus large que les dispositions prévues par la directive concernant les données faisant l'objet d'un tel échange. En effet, le paragraphe (2) du nouvel article 10 bis de la directive 2003/56/CE, introduit par la directive, prévoit que : *« Peuvent figurer sur le réseau des renseignements contenus dans les certificats d'aptitude professionnelle (CAP) ainsi que des informations concernant les procédures administratives relatives aux CAP », alors que le paragraphe (5) du nouvel article 6 bis précité prévoit que « le ministre peut communiquer les données contenues dans la banque de données ».*

Dans un souci de transposition correcte de la directive, la CNPD se demande si une telle formulation ne va pas au-delà des dispositions légales prévues par la directive si elle porte, effectivement, sur un champ plus large de catégories de données pouvant faire l'objet d'un tel échange. Cela reviendrait, en effet, à prévoir un échange de données sur des catégories de données non prévues par la directive.

En outre, une telle formulation pourrait amener, le cas échéant, à ne pas respecter le principe de la limitation des finalités, tel que mentionné ci-avant, ni le principe de minimisation des données[279], alors que pourraient être collectées des catégories de données qui n'ont pas été collectées pour les finalités visées au paragraphe (2), point 3, du nouvel article 6 bis précité ou dont la collecte n'est pas nécessaire aux fins de réalisation de la finalité précitée.

3. Sur la durée de conservation des données à caractère personnel

La Commission nationale regrette que la loi sous avis ne fasse pas mention de la durée de conservation des données à caractère personnel collectées pour les finalités énoncées au paragraphe (2) de l'article 6 bis.

[279] Le principe de minimisation des données signifie que le responsable du traitement doit traiter uniquement les données qui sont nécessaires (et non seulement utiles) à la réalisation des finalités.

Or, conformément à l'article 5 paragraphe (1), lettre e) du RGPD, les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées.

En l'absence de précision sur ce point dans le projet de loi ou dans le commentaire des articles, la CNPD n'est pas en mesure d'apprécier si en l'occurrence, le principe de durée de conservation limitée des données a été respecté concernant la collecte de ces données.

Ainsi décidé à Esch-sur-Alzette en date du 15 novembre 2019.

La Commission nationale pour la protection des données

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

Avis de la Commission nationale pour la protection des données à l'égard des amendements gouvernementaux au projet de règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14quater-1 et 14quater-2 de la loi modifiée du 25 février 1979 concernant l'aide au logement.

Délibération n°54/2019 du 25 novembre 2019

Conformément à l'article 57, paragraphe 1er, lettre (c) du règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») *« conseille, conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement ».*

Faisant suite à la demande lui adressée par Monsieur le Ministre du logement en date du 15 octobre 2019, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet des amendements gouvernementaux :

- au projet de règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14quater-1 et 14quater-2 de la loi modifiée du 25 février 1979 concernant l'aide au logement, et
- au projet de règlement grand-ducal déterminant les critères minimaux de salubrité, d'hygiène, de sécurité et d'habitabilité auxquels doivent répondre les logements et chambres donnés en location ou mis à disposition à des fins d'habitation.

La CNPD limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par les articles 2 et 3 du projet de règlement grand-ducal fixant les mesures d'exécution relatives à l'aide au financement de garanties locatives prévues par les articles 14quater-1 et 14quater-2 de la loi modifiée du 25 février 1979 concernant l'aide au logement (ci-après : « le projet de règlement grand-ducal »). Elle n'entend dès lors pas se prononcer au sujet du projet de règlement grand-ducal déterminant les critères minimaux de salubrité, d'hygiène, de sécurité et d'habitabilité auxquels doivent répondre les logements et chambres donnés en location ou mis à disposition à des fins d'habitation.

Il convient de relever que le projet de règlement grand-ducal a pour origine le projet de loi n°7258, transformé en projet de loi n°7258A portant modification de la loi modifiée du 25 février 1979 concernant l'aide au logement. Ce projet de loi entend notamment introduire des nouveaux articles 14quater-1 et 14quater-2 dans la loi modifiée du 25 février 1979 concernant l'aide au logement, afin d'aligner les dispositions relatives à l'aide au financement de garanties locatives à celles concernant la subvention de loyer.

En date du 14 septembre 2018, la Commission nationale avait émis un avis relatif tant à ce projet de loi, qu'au projet de règlement grand-ducal sous examen (délibération n°450/2018, document parlementaire 7258/03). Elle limite donc ses observations aux changements introduits par les amendements au projet de règlement grand-ducal et renvoie pour le surplus à ses commentaires et suggestions émis à l'occasion de son précédent avis.

***Ad* article 2 du projet de règlement grand-ducal, tel qu'amendé**

Dans son avis du 14 septembre 2018, la CNPD notait que le projet de règlement grand-ducal prévoyait implicitement dans son article 2 les catégories de données qui pourraient être traitées par le ministère du logement aux fins de l'instruction ou du réexamen d'une demande d'aide au financement d'une garantie locative, ainsi que leur origine. Elle regrettait toutefois l'ancienne formulation du paragraphe (2) de cet article 2 (*« Le demandeur fournit, sur demande du ministre, tous renseignements et documents nécessaires à l'instruction de sa demande »*), qui ne lui paraissait guère conforme au principe de prévisibilité auquel doit répondre tout texte légal ou réglementaire et laissait par ailleurs courir le risque que la personne concernée se voit obligée de devoir transmettre davantage de données à caractère personnel en fonction de sa situation particulière, voire de l'appréciation de l'agent du ministère qui serait amené à traiter sa demande (situation qui serait susceptible de contrevenir au principe d'égalité devant la loi, consacré à l'article 10bis de la Constitution).

Suite aux amendements proposés par le Gouvernement sur base de l'observation émise par le Conseil d'État dans son avis du 9 octobre 2018 (avis C.E. no 52.750), l'article 2 paragraphe (2) du projet de règlement grand-ducal se lit maintenant de la façon suivante : *« Au cas où le ministre demande au demandeur des renseignements et documents supplémentaires ou complémentaires et si le demandeur ne les verse pas dans les trois mois, le dossier de demande est clôturé et le demandeur ne pourra pas prétendre à l'aide sollicitée ».*

La Commission nationale regrette néanmoins que cette nouvelle formulation ne réponde pas vraiment à ses remarques formulées dans son avis du 14 septembre 2018, dans la mesure où le projet de règlement grand-ducal ne précise pas quelles sont ces catégories de données, *« renseignements et documents supplémentaires ou complémentaires »* qui peuvent être demandées par le ministre, ce qui pose la question de la transparence vis-à-vis du citoyen désirant obtenir une aide au financement d'une garantie locative, et laisse courir un risque éventuel de traitement arbitraire quant à l'octroi de cette aide.

***Ad* article 3 du projet de règlement grand-ducal, tel qu'amendé**

L'article 3 du projet de règlement grand-ducal prévoyait initialement, dans son paragraphe 1er, second alinéa : *« L'établissement de crédit auprès duquel le demandeur a ouvert un contrat de dépôt conditionné en obtient une copie de la décision d'octroi ou de refus pour information ».*

Le paragraphe 3 de ce même article 3 prenait quant à lui la teneur suivante : *« En cas d'octroi de l'aide, le demandeur est tenu de faire parvenir au ministre sans délai une copie du contrat de dépôt conditionné conclu entre le demandeur et l'établissement de crédit ».*

Les amendements visent à supprimer ces deux dispositions de l'article 3 du projet de règlement grand-ducal.

Selon le commentaire des amendements, il convenait de supprimer l'alinéa 2 du paragraphe 1er *« car la pratique a montré qu'il n'y a aucune utilité pour l'établissement financier d'obtenir une copie de la décision d'octroi ou de refus de l'aide « pour information ».* La Commission nationale salue cet amendement, dans la mesure où il permet d'éviter une transmission inutile, voire disproportionnée, de données à caractère personnel à des tiers, en l'espèce des établissements de crédit.

Quant au paragraphe 3, il ne faisait plus de sens au vu de la condition prévue par l'article 14quater-1, paragraphe 2, point 4° de la loi modifiée du 25 février 1979 concernant l'aide au logement, selon lequel *« l'aide ne peut être accordée que si le demandeur a préalablement ouvert un compte de dépôt conditionné auprès d'un établissement de crédit ».* La Commission nationale comprend donc que la transmission d'une copie du contrat de dépôt au ministre n'était plus nécessaire et estime en effet que cette information ne devrait par conséquent pas être collectée ni traitée par le ministre *après* l'octroi de l'aide au logement.

Elle se demande cependant, dans l'hypothèse où une copie du contrat de dépôt serait collectée auprès du demandeur avant l'octroi de l'aide aux fins de vérifier s'il répond à la condition prévue par l'article 14quater-1, paragraphe 2, point 4° de la loi précitée, s'il ne serait pas opportun de faire figurer cet élément dans les informations à annexer au formulaire de demande, reprises à l'article 2 paragraphe (1) du projet de règlement grand-ducal.

Ainsi décidé à Esch-sur-Alzette en date du 25 novembre 2019.

La Commission nationale pour la protection des données,

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

ANNEXES

5

Avis de la Commission nationale pour la protection des données relatif 1. au projet de loi n°7475 portant modification de la loi modifiée du 26 juillet 2002 sur la police et sur l'exploitation de l'aéroport de Luxembourg ainsi que sur la construction d'une nouvelle aérogare ; 2. au projet de règlement grand-ducal relatif à la sûreté de l'aviation civile et aux conditions d'accès à l'aéroport de Luxembourg.

Délibération n°59/2019 du 17 décembre 2019

Conformément à l'article 57 paragraphe (1) lettre (c) du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après désigné « le RGPD »), ainsi qu'à l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, chaque autorité de contrôle a pour mission de conseiller *« conformément au droit de l'État-membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement. »*

L'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données prévoit précisément que la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») exerce les missions dont elle est investie en vertu de l'article 57 du RGPD, tandis que l'article 8 point 3° de ladite loi du 1er août 2018 se base sur l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n° 2016/680 précitée en prévoyant que la CNPD *« conseille la Chambre des députés, le Gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données personnelles ».*

Par courrier en date du 23 septembre 2019, Monsieur le Ministre de la Mobilité et des Travaux publics a invité la Commission nationale à se prononcer sur le projet de loi n°7475 portant modification de la loi modifiée du 26 juillet 2002 sur la police et sur l'exploitation de l'aéroport de Luxembourg ainsi que sur la construction d'une nouvelle aérogare, d'une part, et sur le projet de règlement grand-ducal relatif à la sûreté de l'aviation civile et aux conditions d'accès à l'aéroport de Luxembourg, d'autre part.

Par courrier en date du 09 décembre 2019, Monsieur le Ministre de la Mobilité et des Travaux publics a invité la Commission nationale à se prononcer sur l'amendement gouvernemental relatif au projet de règlement grand-ducal relatif à la sûreté de l'aviation civile et aux conditions d'accès à l'aéroport de Luxembourg.

Au niveau européen, la sûreté de l'aviation civile est réglementée par le règlement (CE) 300/2008 du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile, ainsi que par le règlement d'exécution (UE) 2015/1998 de la Commission européenne du 5 novembre 2015 en ce qui concerne la clarification, l'harmonisation et la simplification ainsi que le renforcement de certaines mesures de sûreté aérienne spécifiques. Compte tenu des menaces terroristes dans toute l'Europe et du nombre grandissant d'infractions liées à des activités terroristes, la Commission européenne a récemment modifié le règlement (UE) 2015/1998 précité par le règlement d'exécution (UE) 2019/103 du 23 janvier 2019. D'après l'exposé des motifs du projet de loi n°7475, le texte législatif et réglementaire en projet sous examen visent précisément à mettre en œuvre ladite modification du règlement d'exécution 2015/1998 *« en ce qui concerne la clarification, l'harmonisation et la simplification ainsi que le renforcement de certaines mesures de sûreté aérienne spécifique et plus particulièrement des dispositions concernant la vérification des antécédents pour déterminer la fiabilité d'une personne ».*

La Commission nationale entend limiter ses observations aux dispositions des deux projets, y compris aux dispositions de l'amendement gouvernemental relatif au projet de règlement grand-ducal, lui soumis pour avis qui ont une répercussion sur le respect de la vie privée et la protection des données à caractère personnel.

1. Remarques préliminaires

L'article unique du projet de loi n°7475 portant modification de la loi modifiée du 26 juillet 2002 sur la police et sur l'exploitation de l'aéroport de Luxembourg ainsi que sur la construction d'une nouvelle aérogare (ci-après : « le projet de loi ») vise à remplacer l'article premier de la loi précitée du 26 juillet 2002. D'après les auteurs du projet de loi, cet article a pour objet d'opérer deux changements fondamentaux:

- La fiabilité d'une personne n'est plus constatée par un contrôle préalable à l'embauche effectué par l'employeur et, le cas échéant, par une vérification des antécédents effectuée par la Police grand-ducale[280], mais selon les circonstances, par une vérification des antécédents ordinaire, voire même une vérification des antécédents renforcée. Selon le règlement d'exécution 2019/103 de la Commission européenne, les contrôles préalables à l'embauche doivent cesser avant le 31 juillet 2019. Les personnes ayant subi un contrôle préalable à l'embauche doivent faire l'objet d'une vérification des antécédents le 30 juin 2020 au plus tard.

- Un changement des compétences aura lieu en ce sens que même si la Police grand-ducale continuera d'effectuer la vérification des antécédents, il revient au ministre ayant la Police grand-ducale dans ses attributions (ci-après : le « ministre » ou le « ministère ») d'en prendre la décision finale. Les auteurs justifient cette modification par *« la sensibilité et l'importance des décisions à prendre, et afin de renforcer la légalité des actes administratifs relatifs à la vérification des antécédents et ainsi accroître la sécurité juridique, la compétence finale ne devrait plus relever de la Police grand-ducale, mais devra être élevée au niveau ministériel. ».*

[280] Tel que prévu actuellement par l'article 12.3 paragraphe (1), alinéa 4 du règlement grand-ducal du 24 février 2016 relatif aux conditions d'accès à l'aéroport de Luxembourg et aux contrôles de sûreté y applicables.

ANNEXES

5

A titre liminaire, il convient de rappeler que la directive (UE) n°2016/680 du 27 avril 2016[281] (ci-après désignée « la Directive 2016/680 »), établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel qui sont à respecter par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.[282] Comme une directive européenne ne lie les États-membres que quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens[283], ladite Directive 2016/680 laisse clairement une marge de manœuvre au profit des États-membres en son article 1er paragraphe (3) qui précise qu'elle *« n'empêche pas les États-membres de prévoir des garanties plus étendues que celles établies dans la présente directive pour la protection des droits et des libertés des personnes concernées à l'égard du traitement des données à caractère personnel par les autorités compétentes. ».*

Par ailleurs, la Directive 2016/680 dispose que pour être licite, le traitement doit être nécessaire à l'exécution d'une mission de l'autorité compétente, correspondre aux finalités pour lesquelles il a été mis en place, mais aussi et surtout, il doit être prévu soit par le droit de l'Union, soit par le droit d'un État-membre[284]. En outre, la Directive 2016/680 précise que la disposition nationale qui réglemente ledit traitement doit au moins préciser : les objectifs du traitement, les données à caractère personnel devant faire l'objet du traitement et les finalités du traitement[285]. Il ressort de cette disposition que ces trois éléments constituent le seuil minimal qu'une disposition nationale réglementant un traitement tombant dans le champ d'application de la Directive 2016/680 doit respecter. La CNPD tient à renvoyer à ses observations formulées à cet égard dans son avis relatif au fichier central de la Police grand-ducale au regard de la législation sur la protection des données émis le 13 septembre 2019[286].

La Directive 2016/680 a été transposée par le législateur luxembourgeois 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 (ci-après : « la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale »). Dans le commentaire des articles du projet de loi n°7168 devenu la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, les auteurs avaient précisé que le rapport entre le RGPD et la future loi est précisément celui d'une « lex generalis » par rapport à une « lex specialis » en ce sens que tous les traitements de données à caractère personnel relèvent du RGPD *« sauf si deux conditions sont remplies cumulativement : 1) il faut que les données soient traitées par une autorité compétente au sens de la directive (UE) n°2016/680 telle que définie à l'article 3, point 7), du projet de loi sous examen, et 2) il faut que les données soient traitées pour une des finalités visées à l'article 1er du projet de loi. ».*

L'article 6 du RGPD définit les différentes conditions de licéité pour lesquelles un traitement est possible. En d'autres termes, le responsable du traitement doit préalablement et pour chaque traitement de données personnelles,

[281] Directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.
[282] Article 1er paragraphe (1) de la Directive 2016/680.
[283] Prévu par l'article 288, alinéa 3 du Traité sur le fonctionnement de l'Union européenne.
[284] Article 8 paragraphe (1) de la Directive 2016/680.
[285] Article 8 paragraphe (2) de la Directive 2016/680.
[286] Délibération n°45/2019 du 13 septembre 2019.

déterminer la condition de licéité y applicable. En particulier, il convient de rappeler que le traitement de données à caractère personnel collectées et traitées dans le cadre de l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement doit reposer sur une base légale conformément à l'article 6 paragraphe (3) du RGPD, lu ensemble avec son paragraphe (1) lettres c) et e)[287] qui dispose que : *« Le fondement du traitement visé au paragraphe 1, points c) et e), est défini par :*

c. le droit de l'Union; ou

d. le droit de l'État-membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique ou, en ce qui concerne le traitement visé au paragraphe 1, point e), sont nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres: les conditions générales régissant la licéité du traitement par le responsable du traitement; les types de données qui font l'objet du traitement; les personnes concernées; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités; les durées de conservation; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. »

Il résulte de ce qui précède que cet article prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans ces deux cas de figure, le fondement et les finalités des traitements de données doivent spécifiquement être définis soit par le droit de l'Union européenne, soit par le droit de l'État-membre auquel le responsable du traitement est soumis.

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

En vertu des dispositions précitées, ces bases légales devraient établir des dispositions spécifiques visant à déterminer, entre autres, les types de données traitées, les personnes concernées, les entités auxquelles les données peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

[287] L'article 6, paragraphe (1), lettres c) et e) dispose que : *« Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : (…) c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; (…) e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; (…) ».*

Le considérant (41) du RGPD énonce encore que *« cette base juridique ou cette mesure législative devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme. ».*

Ainsi, la Commission nationale se doit de souligner l'importance fondamentale du principe de licéité d'un traitement de données à caractère personnel qui doit être lu à la lumière de l'article 8 paragraphe (2) de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52 paragraphes (1) et (2) de la Charte des droits fondamentaux de l'Union européenne. En substance, ces deux articles, ensemble avec la jurisprudence constante de la Cour européenne des droits de l'Homme, retiennent qu'un traitement de données effectué par une autorité publique peut constituer une ingérence dans le droit au respect de la vie privée ou limiter l'exercice du droit à la protection des données. Cette ingérence ou limitation peut être justifiée à condition qu'elle:

- soit prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante ;
- soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité ;
- respecte le contenu essentiel du droit à la protection des données ;
- réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui.

En ce qui concerne la première condition, selon la jurisprudence de la Cour européenne des droits de l'Homme, une ingérence au droit au respect de la vie privée n'est *« prévue par la loi »,* au sens de l'article 8 paragraphe (2) de la Convention européenne des droits de l'homme[288], que si elle repose sur un article du droit national qui présente certaines caractéristiques. L'expression « prévue par la loi » implique donc notamment que la législation interne doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention[289]. La loi doit être *« accessible aux personnes concernées et prévisible quant à ses répercussions »*[290]. Une règle est prévisible *« si elle est formulée avec une précision suffisante pour permettre à toute personne – bénéficiant éventuellement d'une assistance appropriée – d'adapter son comportement »*[291] ainsi que *« Le degré de précision requis de la "loi" à cet égard dépendra du sujet en question. »*[292].

Afin de remplir ces critères d'accessibilité et de prévisibilité de la loi, d'une part, et ainsi limiter d'éventuels comportements arbitraires et abusifs de la part des autorités publiques, d'autre part, le droit national peut donc prévoir et encadrer plus spécifiquement les traitements de données à caractère personnel effectués par de telles autorités, comme le ministre ou la Police grand-ducale. Cet encadrement légal serait par ailleurs un garant du principe de sécurité juridique au profit des personnes concernées, ainsi que des différents responsables du

[288] L'article 8 paragraphe (2) de la Convention européenne des droits de l'homme dispose que : *« Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».*

[289] CouEDH, Fernández Martinez c. Espagne [GC], n°56030/07, para. 117.

[290] CouEDH, Amann c. Suisse [GC], n°27798/95, 16 février 2000, para. 50 ; voir également CouEDH, Kopp c. Suisse, n°23224/94, 25 mars 1998, para. 55 et CouEDH, Iordachi et autres c. Moldavie, n°25198/02, 10 février 2009, para. 50.

[291] CouEDH, Amann c. Suisse [GC], n°27798/95, 16 février 2000, para. 56 ; voir également CouEDH, Malone c. Royaume-Uni, n°8691/79, 26 avril 1985, para. 66 ; CouEDH, Silver et autres c. Royaume-Uni, n°5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.

[292] CouEDH, The Sunday Times c. Royaume-Uni, n°6538/74, 26 avril 1979, para. 49 ; voir également CouEHD, Silver et autres c. Royaume-Uni, n°5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.

traitement. La sécurité juridique constitue même un principe général du droit de l'Union européenne, exigeant notamment qu'une réglementation entraînant des conséquences défavorables à l'égard de particuliers soit claire et précise et son application prévisible pour les justiciables. La réglementation doit permettre aux intéressés de connaître avec exactitude l'étendue des obligations qu'elle leur impose, doit leur permettre de connaître sans ambiguïté leurs droits et leurs obligations ainsi que leur permettre de prendre leurs dispositions en conséquence[293].

C'est la raison pour laquelle, la Cour européenne des droits de l'homme au sein de sa jurisprudence affirme que *« le droit interne doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par l'article 8 paragraphe 1 »*[294]. Par conséquent, la loi *« doit définir l'étendue et les modalités d'exercice du pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire »*[295]. La Cour de justice de l'Union européenne estime qu'en cas de limitation de la protection des données à caractère personnel ou du droit au respect de la vie privée un texte légal *« doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »*[296].

Par ailleurs, la protection des données à caractère personnel constitue au niveau national une matière réservée à la loi en ce qu'elle touche à la protection de la vie privée des citoyens (article 11 paragraphe (3) de la Constitution). En vertu de l'article 32, paragraphe (3), de la Constitution, dans lesdites matières réservées à la loi par la Constitution, « le Grand-Duc ne peut prendre des règlements et arrêtés qu'en vertu d'une disposition légale particulière qui fixe, outre les objectifs, les principes et points essentiels des mesures d'exécution. »[297].

Les éléments essentiels[298], les objectifs et les principes[299] doivent dès lors figurer dans la loi au sens strict du terme.

Il ne fait aucun doute que les traitements de données effectués par le ministre et la Police grand-ducale dans le cadre des vérifications des antécédents constituent une ingérence dans le droit au respect de la vie privée et le droit à la protection des données, de sorte que les conditions et les modalités de ces traitements doivent obligatoirement être prévues dans la loi.

Ceci étant dit, la CNPD souhaite attirer l'attention sur le fait que le projet de loi lui soumis pour avis devrait nécessairement préciser quelle est la finalité poursuivie par le traitement de données à caractère personnel opéré dans le cadre des vérifications des antécédents et qui a la qualité de responsable du traitement pour les opérations précitées comme expliqué ci-dessous aux points *1.1* et *1.2.* de l'avis. Cette précision est d'autant plus importante

[293] Voir p.ex. Cour EDH, Aurubis Balgaria du 31 mars 2011, C-546/09, points 42-43 ; Arrêt, Alfamicro c. Commission du 14 novembre 2017, T-831/14, points 155-157.
[294] Cour EDH, Amann c. Suisse [GC], n°27798/95 para 56.
[295] *Ibidem.* Voir également Cour EDH, Malone c. Royaume-Uni, série A n°82, du 2 août 1984, pp. 31-32, para.66 ; Cour EDH, Fernández Martínez c. Espagne CE:ECHR:2014:0612JUD005603007, 12 juin 2014 para.117 ; Cour EDH, Liberty et autres c. Royaume-Uni, n°58243/00, du 1er juillet 2008, para. 62 et 63; Cour EDH, Rotaru c. Roumanie, App. n°28341/95, 4 mai 2000, para. 57 à 59 et Cour EDH, S et Marper c. Royaume-Uni, Requêtes n°30562/04 et 30566/04, du 4 décembre 2008 para. 99. ; Dimitrov-Kazakov c. Bulgarie n°11379/03, du 10 février 2011.
[296] Arrêt du 8 avril 2014, Digital Rights Ireland e.a. C-293/12 et C-594/12, EU :C :2014 :238, point 54.
[297] Avis n°52976 du Conseil d'État du 24 juillet 2018 relatif au Projet de règlement grand-ducal 1. modifiant le règlement grand-ducal modifié du 10 août 2005 relatif au fonctionnement du lycée-pilote, et 2. abrogeant le règlement grand-ducal du 27 août 2012 portant sur les classes de la division supérieure de l'enseignement secondaire dans le cycle de formation du lycée Ermesinde.
[298] Arrêt de la Cour constitutionnelle - Arrêts n°00132 et 00133 du 2 mars 2018.
[299] Avis n°52976 du Conseil d'État du 24 juillet 2018 relatif au Projet de règlement grand-ducal 1. modifiant le règlement grand-ducal modifié du 10 août 2005 relatif au fonctionnement du lycée-pilote, et 2. abrogeant le règlement grand-ducal du 27 août 2012 portant sur les classes de la division supérieure de l'enseignement secondaire dans le cycle de formation du lycée Ermesinde.

dans le cadre des deux textes sous avis, car elle entraîne potentiellement l'application d'un cadre juridique différent en matière de protection des données. En effet, tandis que le RGPD s'applique de manière générale au traitement des données à caractère personnel effectué par un responsable du traitement ou un sous-traitant établi sur le territoire de l'Union européenne, la Directive 2016/680 établit des règles spécifiques de protection des données lorsque le traitement est effectué par un responsable du traitement qui agit comme autorité compétente *« 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. »* (article 1er paragraphe (1) de la Directive 2016/680).

1.1. Quant à la finalité poursuivie

En ce qui concerne tout d'abord la finalité poursuivie par le traitement de données à caractère personnel opéré dans le cadre des vérifications des antécédents d'une personne qui est obligée de par la réglementation européenne et nationale de se soumettre à une telle vérification, la CNPD constate que ladite finalité n'est pas précisée dans le corps des projets de textes. Or, elle est d'avis qu'il ressort de l'économie générale du règlement d'exécution 2015/1998 modifié par le règlement 2019/103 de la Commission européenne, règlement que les deux textes sous examen visent à mettre en œuvre, que ces vérifications visent à renforcer la sécurité sur les aéroports ce qui peut être considéré comme une mesure de prévention contre les menaces pour la sécurité publique. En effet, en raison de l'évolution récente des technologies et équipements de sûreté, nécessaires afin de faire face aux nouveaux visages de la menace terroriste, il est d'autant plus important que les personnes travaillant dans la zone aéroportuaire fournissent un degré d'assurance et de fiabilité élevé, tout en possédant les capacités et aptitudes physiques et mentales requises pour s'acquitter de manière efficace des tâches qui leur sont confiées. La Commission européenne a précisément estimé que les modifications des normes de base communes dans le domaine de la sûreté aérienne concernent, entre autres, *« la révision des règles relatives à la vérification des antécédents afin de renforcer la culture de la sûreté et la résilience. »*[300].

Ainsi, sur base des considérations susmentionnées et sans explications supplémentaires par les auteurs du projet de loi, la CNPD est d'avis que la finalité poursuivie par le traitement de données à caractère personnel effectué dans le cadre des vérifications des antécédents entre a priori dans le champ d'application matériel de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale. Comme susmentionné, elle recommande aux auteurs de préciser la finalité poursuivie par le traitement de données à caractère personnel dans le corps du texte du projet de loi.

Or, encore faut-il que la deuxième condition dudit champ d'application, tel que mentionné plus haut, soit remplie, c'est-à-dire le traitement de données à des fins pénales et de sécurité nationale doit être mis en œuvre par *« toute autorité publique compétente ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique »*[301]. C'est précisément à cet égard que la définition du

[300] Considérant (4) du règlement d'exécution 2019/103 de la Commission du 23 janvier 2019.
[301] Article 1 paragraphe (1) de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale.

responsable du traitement joue un rôle crucial et la CNPD se permet de relever les potentielles configurations en la matière avec les implications et problématiques que ces dernières peuvent engendrer au niveau législatif. Or, faute de précision dans les projets de textes, elle ne peut qu'esquisser différentes options.

1.2. Quant au responsable du traitement

D'après la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, le responsable du traitement est l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel[302]. En vertu du RGPD, le responsable du traitement est défini comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui détermine seul ou conjointement avec d'autres les finalités et les moyens du traitement[303].

Tout d'abord, comme la fiabilité d'un employé futur de l'aéroport n'est plus constatée par un contrôle préalable à l'embauche effectué par l'employeur, qui semble être en espèce la société de l'Aéroport de Luxembourg (la société dite « lux-Airport »)[304], celle-ci ne peut pas être considérée comme responsable du traitement des données effectué dans le cadre des vérifications des antécédents.

Ensuite, il est important de rappeler que le ministre ayant la Police grand-ducale dans ses attributions assure la responsabilité finale de la Police grand-ducale en matière de décisions concernant l'octroi ou le refus d'une vérification des antécédents. Si la Police grand-ducale est actuellement compétente pour prendre les décisions relatives aux vérifications des antécédents, le projet de loi transfère cette compétence dorénavant au ministre. En effet, le commentaire de l'article unique paragraphe (2) du projet de loi mentionne expressément que *« vu la sensibilité et l'importance de ces décisions, il a été décidé d'un commun accord entre les entités concernées que la compétence finale en matière de vérification des antécédents ne devra plus relever de la Police grand-ducale, mais devra être élevée au niveau ministériel, et le Ministère de la Sécurité intérieure a été identifié comme ministère le plus approprié pour assumer cette mission. ».*

Ainsi, faute de précision dans le texte du projet de loi, il n'est pas évident d'identifier le ou les responsable(s) du traitement au sens de l'article 4 point 7) du RGPD et de l'article 2 point 8 de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale. Il est donc primordial de connaître plus en détail les opérations du traitement de données en question. Quelles données et informations la Police grand-ducale continue-t-elle au ministre et sur base de quels éléments ce dernier va prendre sa décision suite à une demande de vérification des antécédents ? Est-ce que la Police se contente de regrouper de manière objective toutes les informations trouvées sur la personne ayant introduite une demande de vérification et de les envoyer au ministre ou effectue-t-elle déjà une première évaluation desdites informations ? En fonction des réponses à ces questions, développées encore plus en détail sous le point *« Ad. Art. 13. Demande de vérification des antécédents »,* trois différentes hypothèses sont envisageables :

[302] Article 2 paragraphe (1) point 8° de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale.
[303] Article 4 point 7 du RGPD.
[304] Il s'agit de l'organisme désigné en vertu de la loi modifiée du 26 juillet 2002 sur la police et sur l'exploitation de l'aéroport de Luxembourg ainsi que sur la construction d'une nouvelle aérogare de l'exploitation de l'Aéroport de Luxembourg.

1. Le ministre pourrait être considéré comme responsable du traitement des données effectué dans le cadre de la décision finale, alors que la Police grand-ducale serait responsable du traitement des données effectué dans le cadre de la vérification-même des antécédents. Dans l'hypothèse où le ministre serait à considérer comme autorité compétente au sens de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, les deux opérations de traitement de données tomberaient sous le champ d'application de ladite loi du 1er août 2018, la Police étant clairement à qualifier comme une telle autorité compétente au sens de cette loi. Si le ministre ne serait pas à considérer comme « autorité compétente » au sens de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, le traitement effectué par lui tomberait dans le champ d'application du RGPD, ce qui ne serait pas judicieux au vu des finalités poursuivies qui tombent clairement dans le champ d'application de ladite loi. La CNPD recommande ainsi aux auteurs du projet de loi de prévoir dans la loi que le ministre est à considérer comme autorité compétente au sens de l'article 2 paragraphe (1) point 7 de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale. L'article 2 paragraphe (1) point 8° de la loi précitée du 1er août 2018 prévoit même expressément que si *« les finalités et les moyens du traitement de données sont déterminés par le droit de l'Union européenne ou le droit luxembourgeois, le responsable du traitement ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union européenne ou le droit luxembourgeois. »*

2. La notion de « responsabilité conjointe » introduite par l'article 20 de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale[305], pourrait aussi être prise en compte dans ce contexte. La Commission nationale est d'avis qu'il pourrait, le cas échéant, ressortir de l'économie générale des deux textes lui soumis que le ministre d'un côté, et la Police grand-ducale de l'autre côté, participent conjointement à la réalisation des finalités et des moyens du traitement de données à caractère personnel opéré dans le cadre des vérifications des antécédents.

3. Il pourrait aussi être envisagé que la Police grand-ducale agisse en tant que sous- traitant du ministre, au cas où le ministre puisse être qualifié comme autorité compétente au sens de l'article 2 paragraphe (1) point 7 de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale.

La CNPD recommande donc aux auteurs du projet de loi de préciser dans le corps du texte du projet de loi qui a la qualité de responsable du traitement et, le cas échéant, de sous-traitant, en matière de vérifications des antécédents.

2. <u>Quant au projet de règlement grand-ducal relatif à la sûreté de l'aviation civile et aux conditions d'accès à l'aéroport de Luxembourg, tel que modifié par l'amendement gouvernemental du 09 décembre 2019</u>

Le projet de règlement grand-ducal relatif à la sûreté de l'aviation civile et aux conditions d'accès à l'aéroport de Luxembourg, tel que modifié par l'amendement gouvernemental du 09 décembre 2019 (ci-après : le « projet de règlement grand-ducal ») vise à abroger le règlement grand-ducal du 24 février 2016 relatif aux conditions d'accès

[305] Article 20 de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale dispose que : *« (1) Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect de la loi, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 11 et 12, par voie d'accord entre eux. Le point de contact unique pour les personnes concernées, afin que celles-ci puissent exercer leurs droits, est désigné dans l'accord. (2) Indépendamment des termes de l'accord visé au paragraphe 1er, la personne concernée peut exercer les droits que lui confère la présente loi à l'égard de et contre chacun des responsables du traitement. »*

à l'aéroport de Luxembourg et aux contrôles de sûreté y applicables (ci-après : « le règlement grand-ducal du 24 février 2016 ») et à aligner la législation nationale existante au cadre européen actuel.

Ad art. 6. Le laissez-passer journalier

L'article 6 paragraphe (3) du projet de règlement grand-ducal prévoit qu'un laissez-passer journalier est délivré par lux-Airport en échange d'une pièce officielle d'identification émise par les autorités luxembourgeoises ou étrangères. Comme lux-Airport ne devrait a priori pas être considéré comme « autorité compétente » au sens de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, le traitement effectué par ladite société devrait tomber dans le champ d'application du RGPD. La CNPD tient à souligner dans ce contexte l'importance du principe de minimisation des données prévu à l'article 5 paragraphe (1) lettre c) du RGPD, prévoyant que les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. La CNPD comprend dans ce contexte que la carte d'identité est conservée jusqu'à remise du laissez-passer. Or, elle doute que le fait de demander en échange du laissez-passer journalier la remise d'un document d'identité est proportionnel et nécessaire, surtout si on prend en compte l'article 15 paragraphe (1) de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques prévoyant que la carte d'identité est *« obligatoire à partir de l'âge de quinze ans pour les ressortissants luxembourgeois qui résident habituellement dans une commune sur le territoire du Luxembourg et est exigible à toute réquisition de la Police grand-ducale. »* Il découle implicitement de cet article que tous les résidents luxembourgeois âgés de 15 ans et plus doivent à tout moment pouvoir s'identifier au moyen de leur carte d'identité.

En plus des dispositions de l'article 6 paragraphe (3) du projet de règlement grand-ducal, le paragraphe (4) dudit article prévoit que l'identité du titulaire du laissez-passer journalier et de son accompagnateur, ainsi que les heures d'entrée et de sortie sont consignées dans un répertoire tenu au point d'entrée des zones de sûreté aéroportuaires. La CNPD considère qu'au vu du principe de minimisation des données, il apparaît dès lors excessif de conserver le document pendant le temps de présence de la personne en cause dans la zone aéroportuaire, alors que lux-Airport n'est pas en mesure de vérifier si le document d'identité est, le cas échéant, falsifié, et qu'il serait suffisant, après vérification de l'identité de la personne à l'aide de la pièce d'identité, d'ajouter le numéro du document d'identité dans le répertoire précité à côté de l'inscription du titulaire du laissez-passer.

Par ailleurs, il échet de constater que le projet de texte ne prévoit pas cette exigence d'échanger un document d'identité contre un laissez-passer zone délimitée sur base de l'article 8 du projet de règlement grand-ducal et dont la validité est de trois mois. En effet, ledit article ne fait que préciser que l'identité du porteur et de son accompagnateur, ainsi que les heures d'entrée et de sortie sont consignées dans un répertoire tenu aux postes d'entrée aux zones délimitées, ce qui semble être en conformité avec le principe précité de la minimisation des données.

La même remarque s'impose pour l'article 9 du projet de règlement grand-ducal concernant le laissez-passer pour véhicules, qui prévoit qu'il peut être délivré en échange de la carte grise de la voiture ou du permis de conduire du chauffeur. De nouveau, au vu du fait que lux-Airport n'est pas en mesure de vérifier si le permis de conduire ou la carte grise sont, le cas échéant, falsifiés, et en prenant en compte le principe de minimisation des données, il apparaît excessif de conserver les documents en cause. Il paraît suffisant de noter dans le répertoire qui est tenu au point d'entrée des zones délimitées en vertu de l'article 9 paragraphe (3) alinéa 2 du projet de règlement grand-ducal, à côté de l'inscription du titulaire d'un laissez-passer pour véhicules et des heures d'entrée et de sortie, le numéro du permis de conduire, respectivement le numéro d'identification du véhicule qui figure sur la carte grise.

Ad art. 7. Les visiteurs et la presse

Selon l'article 7 du projet de règlement grand-ducal, les visiteurs et les membres de la presse désirant procéder à des prises de vues peuvent se voir délivrer un laissez-passer journalier, sous condition de l'octroi d'une autorisation spécifique préalable par la Police grand-ducale. Le commentaire de l'article en question mentionne à cet égard que comme *« les visiteurs et les membres de la presse ne disposent pas de véritable besoin opérationnel dans le sens d'une activité aéroportuaire, mais que leurs visites correspondent néanmoins à une raison légitime selon la réglementation européenne, ils nécessitent une autorisation spécifique préalable de la part de la Police grand-ducale avant de pouvoir demander un laissez-passer journalier. ».*

L'article 20 du règlement grand-ducal du 24 février 2016, règlement qui sera abrogé par le présent projet, prévoit déjà que les visiteurs et les membres de la presse, désirant procéder à des prises de vues à l'intérieur de l'enceinte aéroportuaire, peuvent se voir accorder par la Police grand-ducale une autorisation d'accéder aux zones de sûreté aéroportuaires. Néanmoins, ni l'article 20 du texte règlementaire actuel, ni l'article 7 du projet de règlement grand-ducal sous avis ou son commentaire ne précisent sur base de quels critères la Police grand-ducale prendra la décision si oui ou non elle délivrera cette autorisation et si, le cas échéant, elle consultera des fichiers nationaux ou des systèmes d'information européens et internationaux comme le système d'information Schengen, le système d'information de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) ou de l'Organisation internationale de police criminelle (INTERPOL) pour prendre la décision susmentionnée. La CNPD tient à renvoyer dans ce contexte à ses commentaires formulés sous le point *« Ad. Art. 13. Demande de vérification des antécédents ».*

En outre, il serait important de savoir si d'autres données à caractère personnel que celles mentionnées à l'article 7, alinéa 2 du projet de règlement grand-ducal seront traitées dans le cadre de cette procédure et ce qu'il advient des données traitées des visiteurs et membres de la presse une fois que l'autorisation par la Police a été accordée ou non. Est-ce que la Police grand-ducale va créer un nouveau fichier propre avec les données à caractère personnel collectées dans le cadre des autorisations en cause ? Si tel est le cas, se pose notamment la question de savoir qui aura accès aux données et combien de temps elles seront conservées.

Il ressort par ailleurs implicitement du texte de l'article 7 du projet de règlement grand-ducal que le ministre n'est pas impliqué dans la procédure des autorisations spécifiques à accorder, le cas échéant, par la Police grand-ducale aux visiteurs et membres de la presse qui en font la demande. Ainsi, il apparaît qu'en vertu de l'article 2 paragraphe (1) point 8 de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, la Police est à considérer comme responsable des traitements de données opérés dans le cadre desdites autorisations. La CNPD recommande donc aux auteurs de le préciser dans le corps du texte du projet sous avis.

Finalement, la CNPD a constaté que, contrairement à l'article 6 du règlement grand-ducal sous avis, son article 7 ne précise pas qui est responsable pour délivrer les laissez-passer journaliers pour les visiteurs et la presse. Est-ce qu'il s'agit de la société lux-Airport ? L'article 8 du projet de règlement grand-ducal prévoit dans ce contexte que les laissez-passer zone délimitée peuvent être délivrés par le responsable sûreté de chaque entité présente dans les zones délimitées. Est-ce que ces entités appartiennent dans leur ensemble à lux-Airport ou est-ce que d'autres sociétés seront présentes dans la zone aéroportuaire et qui seraient alors, le cas échéant, compétentes en la matière ? Si tel est le cas, la Commission nationale recommande de le préciser plus clairement dans le projet de texte règlementaire.

Ad. Art. 13. Demande de vérification des antécédents

1. La collecte initiale des données à caractère personnel par la Police grand-ducale

Selon l'article 13 paragraphe (2) du projet de règlement grand-ducal, une demande de vérification des antécédents est introduite par le requérant auprès de la Police grand-ducale et non pas auprès du ministre. Suite à une telle demande, la Police grand-ducale recueillera différentes données à caractère personnel directement auprès des requérants (une collecte dite « directe » des données) (1.1.), mais elle procèdera aussi à des collectes dites « indirectes » des données (1.2.).

1.1. La collecte directe de données à caractère personnel par la Police grand-ducale

L'alinéa 3 du paragraphe (2) de l'article 13 du projet de règlement grand-ducal énumère en douze points quels éléments une demande de vérification des antécédents doit contenir. La Police grand-ducale reçoit donc directement des personnes en cause les données à caractère personnel figurant dans une telle demande, comme par exemple l'identité du requérant, une liste des lieux de résidences des cinq dernières années ou encore un extrait du bulletin n°3 du casier judiciaire.

La CNPD constate que le règlement modifié d'exécution 2015/1998 ne contient pas de liste à cet égard et elle salue ainsi le degré de détail avec lequel les auteurs du projet de règlement grand-ducal précisent les données à caractère personnel que ladite demande doit contenir. Pour ce qui est de l'exigence d'ajouter à la demande *« un questionnaire*

biographique dûment rempli », la CNPD se demande toutefois quelles données à caractère personnel, en sus de celles déjà énumérées audit article 13 paragraphe (2) du projet de règlement grand-ducal, les demandeurs doivent fournir.

1.2. La collecte indirecte de données à caractère personnel par la Police grand-ducale

En sus des informations collectées directement auprès des demandeurs et faute de précisions dans le texte du projet de règlement grand-ducal, la CNPD se demande si la Police grand-ducale procédera aussi à une collecte indirecte et quelles sont les sources de cette collecte indirecte de données. Il convient de scinder l'analyse de cette question en deux, en visant d'abord la vérification ordinaire des antécédents (1.2.1) et ensuite la vérification renforcée des antécédents (1.2.2). La CNPD abordera ensuite, à défaut de précisions dans le texte du projet de règlement grand-ducal, la question de la durée de validité des différentes vérifications des antécédents (1.2.3.).

1.2.1. La vérification ordinaire des antécédents

Selon l'article 11.1.2 du règlement d'exécution 2019/103, les États-membres peuvent décider de soumettre les personnes recrutées pour mettre en œuvre ou être responsables de la mise en œuvre de l'inspection/filtrage, du contrôle d'accès ou d'autres contrôles de sûreté *« ailleurs que dans une zone de sûreté à accès réglementé, ou disposant d'un accès non accompagné au fret aérien et au courrier aérien, au courrier des transporteurs aériens et au matériel des transporteurs aériens, aux approvisionnements de bord et aux fournitures destinées aux aéroports qui ont fait l'objet des contrôles de sûreté requis »* soit à une vérification ordinaire des antécédents, soit renforcée. Les auteurs du projet de règlement grand-ducal ont opté dans ce cas pour une vérification des antécédents ordinaire (article 14 du projet de règlement grand-ducal).

L'article 13 paragraphe (3) alinéa 2 du projet de règlement grand-ducal précise que toute vérification ordinaire des antécédents doit établir l'identité de la personne sur la base de documents, prendre en considération le casier judiciaire dans tous les États de résidence au cours des cinq dernières années, ainsi que les emplois, les études et les interruptions au cours des cinq dernières années. Ladite vérification doit par ailleurs tenir compte des infractions mentionnées au paragraphe (4) de l'article en cause.

Il ressort a priori des dispositions susmentionnées du projet de règlement grand-ducal que la liste des éléments à prendre en compte par la Police grand-ducale dans le cadre d'une vérification ordinaire des antécédents est à considérer comme exhaustive, c'est-à-dire que la Police grand-ducale ne devrait pas prendre en compte d'autres informations qui lui sont directement ou indirectement disponibles ou accessibles.

1.2.2. La vérification renforcée des antécédents

Le paragraphe (3) alinéa 1er de l'article 13 du projet de règlement grand-ducal énumère quels éléments la vérification renforcée des antécédents doit contenir. Tout comme la vérification ordinaire, la vérification renforcée des antécédents doit tout d'abord permettre d'établir l'identité de la personne sur la base de documents, prendre en considération le casier judiciaire dans tous les États de résidence au cours des cinq dernières années, les emplois, les études et les interruptions au cours des cinq dernières années et prendre en compte les infractions mentionnées audit paragraphe (4). Or, à la différence de la vérification ordinaire, une vérification renforcée des antécédents doit prendre en considération en plus des éléments précités *« les informations des services de renseignement et toute autre information pertinente dont les autorités nationales compétentes disposent et estiment qu'elles peuvent présenter un intérêt pour apprécier l'aptitude d'une personne à exercer une fonction qui requiert une vérification renforcée de ses antécédents. »*

La CNPD constate que tous ces éléments sont repris textuellement du point 11.1.3 de l'annexe du règlement d'exécution 2015/1998 tel que modifié par le règlement d'exécution 2019/103 de la Commission européenne. Elle souhaite à cet égard formuler des observations liées à deux différentes problématiques :

- 1. l'éventuel accès de la Police grand-ducale à ses fichiers nationaux et aux systèmes d'information européens et internationaux ;
- 2. les informations des services de renseignement et *« toute autre information pertinente dont les autorités nationales compétentes disposent ».*

Les remarques concernant le premier point sont aussi pertinentes pour les demandes de vérification ordinaire des antécédents, mais elles ont une plus grande importance pour la vérification renforcée qui apparaît encore plus intrusive pour les droits et libertés des personnes concernées que la vérification ordinaire.

1ère problématique: les éventuels accès de la Police grand-ducale

Il ressort de l'article 13 paragraphe (3) du projet de règlement grand-ducal que la liste des éléments à prendre en considération dans le cadre d'une vérification renforcée des antécédents ne semble pas être exhaustive, car il y est prévu que *« toute vérification renforcée des antécédents doit au moins […] »* prendre en compte lesdits éléments. Cette formulation a aussi été reprise mot par mot du règlement d'exécution de la Commission euopéenne précité. Il ne ressort pas clairement du projet du texte règlementaire sous avis si la Police grand-ducale entend dans le cadre d'une demande de vérification renforcée des antécédents accéder aux données à caractère personnel contenues dans ses propres fichiers ou traitements de données nationaux (au nombre de 62[306]), comme par exemple le fichier dit « central »,[307] le « fichier stupéfiants »[308] le « fichier des avertissements taxés »[309], etc.,

[306] Comme révélé dans un article d'actualité intitulé « 62 TYPES DE FICHIERS » publié le 7 novembre 2019 sur le site de la Chambre des députés : https://www.chd.lu/wps/portal/public/Accueil/Actualite/ALaUne/?current=true&urile=wcm%3Apath%3Aactualite.public.chd.lu/ST-www.chd.lu/sa-actualites/3532ef0a-6f63-45c6-9894-186e876dd120 (consulté en dernier lieu le 5 décembre 2019).

[307] D'après la réponse commune de monsieur le ministre ayant la Police grand-ducale dans ses attributions François BAUSCH et de monsieur le ministre de la Justice Félix BRAZ à la question parlementaire n°752 du 4 juin 2019 le *« fichier dit « central » comporte tous les procès-verbaux et rapports rédigés par les officiers et agents de police Judiciaire dans le cadre de leur mission de police judiciaire. »*

[308] Qui d'après la réponse du ministre ayant la Police grand-ducale dans ses attributions à question N°1190 du 10 septembre 2019 concernant le fichier en matière de stupéfiants auprès de la Police grand-ducale contient *« des informations pertinentes en matière de lutte contre le trafic illicite de stupéfiants qui peuvent ou non être des données à caractère personnel. »*

[309] D'après la réponse de monsieur le ministre ayant la Police grand-ducale dans ses attributions François BAUSCH à la question parlementaire n°1068 du 16 août 2019, le *« fichier des avertissements taxés (AT) a été créé dans le cadre du règlement grand-ducal du 21 décembre 2004 portant autorisation de la création d'un fichier des personnes ayant subi un avertissement taxé en matière de circulation routière et modification du règlement grand-ducal du 7 juin 1979 déterminant les actes, documents et fichiers autorisés à utiliser le numéro d'identité des personnes physiques et morales. »*

ainsi qu'aux données issues des systèmes d'information européens et internationaux comme les systèmes d'information précités Schengen, Europol ou INTERPOL. Au vu des inquiétudes récentes des citoyens quant au respect des libertés publiques et la protection de leurs données personnelles dans le domaine policier et judiciaire, il est d'autant plus important que des clarifications sur les accès aux fichiers et systèmes susmentionnés se retrouvent au niveau de la loi au sens formel, donc dans le projet de loi n°7475 également sous avis, surtout si on considère le communiqué du 22 juillet 2019 du ministère ayant la Police grand-ducale dans ses attributions sur la refonte complète de la législation nationale relative à la vérification des antécédents à l'aéroport de Luxembourg qui précise ce qui suit : *« Vu la complexité du dossier, bon nombre de questions se posent et doivent être tranchées, notamment dans le contexte de l'accès au fichier central de la Police et de la conservation des données. »*[310].

En France, les articles L. 6342-2 et L. 6342-3 du Code des transports précisent que les accès aux zones de sûreté à accès règlementé d'un aérodrome sont soumis à une habilitation qui est précédée d'une enquête administrative donnant lieu, le cas échéant, à consultation du bulletin n°2 du casier judiciaire et des traitements automatisés de données à caractère personnel gérés par les services de police et de gendarmerie nationales relevant des dispositions de l'article 31 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification. D'après ledit article, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État et qui soit intéressent la sûreté de l'État, la défense ou la sécurité publique, soit ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté, incluant ainsi les traitements opérés par les services de police et de gendarmerie nationales, doivent être autorisés par arrêté du ou des ministres compétents, pris après publication d'un avis motivé de la Commission nationale de l'informatique et des libertés (l'homologue français de la CNPD). Lesdits traitements sont ainsi tous encadrés légalement, comme par exemple le fichier des antécédents judiciaires[311], le fichier d'analyse sérielle[312] ou encore le fichier des personnes recherchées[313].

Par ailleurs, se pose la question de savoir si la Police grand-ducale procèdera au contrôle de l'exactitude et de la véracité des indications des demandeurs concernant leurs emplois, études et interruptions au cours des cinq dernières années. La CNPD se demande ainsi si la Police accédera, le cas échéant, au fichier relatif aux affiliations des salariés, des indépendants et des employeurs géré par le Centre commun de la sécurité sociale sur base de l'article 413 du Code de la Sécurité sociale qui lui est accordé par l'article 43 point 2° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale et si, en sus, elle accédera dans ce contexte à d'autres bases de données que celles mentionnées audit article 43, comme par exemple la base de données de l'Agence pour le développement de l'emploi (ADEM). Il serait aussi pertinent de savoir comment la Police grand-ducale vérifiera, le cas échéant, l'exactitude des données indiquées par les travailleurs non-résidents dans leurs demandes. A priori, comme la Police grand-ducale ne dispose pas d'accès aux fichiers correspondants des pays étrangers, ce contrôle peut paraître moins efficace et moins intrusif que celui pour les travailleurs résidents.

[310] Communiqué par le ministère ayant la Police grand-ducale dans ses attributions du 22 juillet 2019 disponible sur le site internet du gouvernement : https://gouvernement.lu/fr/actualites/toutes_actualites/articles/2019/07-juillet/22-bausch-legislation-aeroport.html (accédé en dernier lieu le 17 octobre 2019).
[311] Prévu par les articles 230-6 à 11 du Code de procédure pénale français.
[312] Prévu par les articles 230-12 à 18 du Code de procédure pénale français.
[313] Prévu par l'article 230-19 du Code de procédure pénale français.

2ème problématique : les services de renseignement et les « autorités nationales compétentes »

L'article 13 paragraphe (3), point 4° du projet de règlement grand-ducal prévoit que toute vérification renforcée des antécédents doit *« prendre en considération les informations des services de renseignement et toute autre information pertinente dont les autorités nationales compétentes disposent et estiment qu'elles peuvent présenter un intérêt pour apprécier l'aptitude d'une personne à exercer une fonction qui requiert une vérification renforcée de ses antécédents. »*. Cette disposition est reprise intégralement de l'article 11.1.3 lettre d) de l'annexe du règlement d'exécution 2019/103 de la Commission européenne et le commentaire des articles reste totalement muet à cet égard. Or, la Commission nationale souhaite mettre en exergue trois points.

Tout d'abord, même si l'article en question mentionne les services de renseignement au pluriel, la Commission nationale comprend qu'au niveau national est visé uniquement le Service de renseignement de l'État réglementé par la loi modifiée du 5 juillet 2016. L'article 9 de ladite loi prévoit même expressément en son paragraphe (2) que le Service de renseignement de l'État *« communique dans les meilleurs délais les renseignements collectés dans le cadre de ses missions aux autorités judiciaires, aux services de la police grand-ducale et aux administrations dans la mesure où ces renseignements paraissent utiles à l'accomplissement de leurs missions respectives. »* Pour éviter toute ambiguïté, la CNPD recommande aux auteurs de remplacer dans le texte les mots « les services de renseignement » par « le Service de renseignement de l'État ».

Ensuite, le point 4° sous revue mentionne que la Police grand-ducale doit prendre en compte *« toute autre information pertinente dont les autorités nationales compétentes disposent »*. Il paraît indispensable pour la CNPD que le texte précise quelles sont les entités visées par les termes susmentionnés « les autorités nationales compétentes ». En effet, il ne devrait pas y avoir de difficultés pour identifier les autorités compétentes dans ce contexte. A titre de comparaison, la loi allemande concernant la sécurité aérienne (*« Luftsicherheitsgesetz »*) énumère en sa section 7 paragraphe (3) quelles autorités nationales l'administration de la sûreté du transport aérien (*« Luftsicherheitsbehörde »*) peut contacter dans le cadre d'une vérification des antécédents et pour autant que ceci soit nécessaire pour l'évaluation de la fiabilité de la personne en cause[314].

Sur base de la section 2 de la loi modifiée du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière, la transmission de données à caractère personnel et d'informations de la Police grand-ducale aux autres administrations de l'État est possible, si une loi autorise ce transfert et si les autres conditions cumulativement prévues à l'article 24 de ladite loi sont respectées. Or, il ne ressort pas clairement de l'article 13 paragraphe (4) du projet de règlement grand-ducal s'il vise effectivement la transmission de données de la Police grand-ducale vers ces autorités nationales compétentes, ou plutôt l'inverse, c'est-à-dire le transfert de données desdites autorités vers la Police grand-ducale. Dans les amendements gouvernementaux du 1er août 2017, les auteurs du projet de loi n°6976 devenu la loi du 22 février 2018 précitée ont précisé que la section 2 vise uniquement les *« transmissions « à sens unique », c'est-à-dire de la part de la Police grand-ducale vers des*

[314] Il s'agit des autorités suivantes : *« Polizeivollzugs- und den Verfassungsschutzbehörden der Länder sowie, soweit im Einzelfall erforderlich, dem Bundeskriminalamt, dem Zollkriminalamt, dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst, dem Militärischen Abschirmdienst und der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik. »*

administrations de l'État – la transmission des données et informations dans l'autre sens étant d'ores et déjà prévue par l'article 23, paragraphe 2, du Code de procédure pénale. ». Or, comme les autorités compétentes n'auront pas connaissance si une personne déterminée a introduit une demande de vérification des antécédents auprès de la Police grand-ducale, cette dernière devra les contacter de sa propre initiative. Ainsi, il apparaît nécessaire d'inclure dans le projet de règlement grand-ducal une liste qui détermine les autorités que la Police grand-ducale devra contacter systématiquement en cas de réception d'une demande de vérification des antécédents.

Pour conclure et résumer les observations relatives à cette partie, la CNPD estime que le projet de loi n°7475 devrait préciser les éventuels accès de la Police grand-ducale à ses propres fichiers, à d'autres fichiers nationaux et aux systèmes d'information européens et internationaux dans le cadre des vérifications des antécédents. Le projet de règlement grand-ducal devrait également indiquer quelles sont les entités visées par les termes « les autorités nationales compétentes », ainsi que les conditions et modalités du transfert de données de ces autorités vers la Police grand-ducale.

1.2.3. La durée de validité des différentes vérifications des antécédents

Par ailleurs, selon l'alinéa 2 du paragraphe (2) de l'article 13 du projet de règlement grand-ducal sous avis, le titulaire d'une décision positive relative à la vérification des antécédents doit introduire une demande de renouvellement au moins trois mois avant la fin de validité de la vérification des antécédents actuelle. Le point 11.1.7 de l'annexe au règlement d'exécution 2015/1998 de la Commission européenne du 5 novembre 2015, tel que modifié par le règlement d'exécution 2019/103 de la Commission européenne du 23 janvier 2019, laisse en effet le choix aux États-membres soit de mettre en place un mécanisme de contrôle continu des éléments examinés dans le cadre d'une vérification ordinaire et renforcée des antécédents grâce à la notification rapide à « l'autorité compétente, à l'exploitant ou à l'entité de délivrance, selon le cas, de tout événement susceptible d'avoir une incidence sur la fiabilité de la personne concernée », soit de prévoir un renouvellement à intervalles réguliers ne dépassant pas douze mois pour les vérifications renforcées des antécédents et trois ans pour les vérifications ordinaires des antécédents. Ce n'est qu'en lisant le commentaire des articles qu'on comprend que les auteurs ont l'intention de reprendre lesdites durées de validité, et que donc la vérification des antécédents ordinaires a une durée de validité de 3 ans, tandis que la vérification renforcée expire déjà après 12 mois.

2. Les critères à prendre en compte par la Police grand-ducale pour émettre son avis

Le texte du projet de règlement grand-ducal ne précise nulle part quels critères ou quel degré de gravité des antécédents sont pris en compte par la Police grand-ducale pour apprécier une demande de vérification des antécédents, c'est-à-dire pour émettre son avis en la matière. La CNPD s'interroge notamment si toute inscription au casier judiciaire par exemple entraîne automatiquement une appréciation négative en matière de vérification des antécédents ou si, par contre, les inscriptions doivent avoir atteint un certain niveau de gravité. La loi allemande

précitée concernant la sécurité aérienne prévoit par exemple en sa section 7 paragraphe (1a) qu'une personne n'a pas atteint le niveau de fiabilité requis si, entre autres, elle a été condamnée lors des dernières dix années à une peine d'emprisonnement d'au moins un an.

A titre de comparaison, il convient de relever que l'article 26 de la loi modifiée du 8 juillet 2018 sur la Police grand-ducale confère une nouvelle mission à la Police grand-ducale, qui consiste à réaliser sur demande des vérifications de sécurité du personnel externe des institutions, organes et organismes de l'Union européenne qui ont leur siège au Luxembourg, comme par exemple la Cour de Justice de l'Union européenne, la Cour des Comptes européennes ou encore la Banque européenne d'investissement. L'article 3 du règlement grand-ducal du 28 juillet 2018 portant exécution dudit article 26 de la loi du 18 juillet 2018 sur la Police grand-ducale prévoit que ces vérifications de sécurité sont réalisées sur base de critères ciblés et spécifiques, indiqués par l'institution, l'organe ou l'organisme requérant en concertation avec la Police. La disposition en question précise qu'au *« terme de la vérification la Police émet un avis basé sur les critères visés à l'alinéa 1er qu'elle transmet à l'institution, organisme ou organe pour le compte de laquelle la vérification a été faite »*. Dans le commentaire des articles, les auteurs dudit règlement grand-ducal ont expliqué que cette disposition vise précisément à assurer que la Police n'ait à répondre que par rapport à l'existence des critères d'exclusion préalablement fixés.

Afin d'éviter l'arbitraire et de respecter le principe de transparence vis-à-vis des demandeurs d'une vérification ordinaire et renforcée des antécédents, le texte du projet de règlement grand-ducal devrait aux yeux de la CNPD définir en détail quels sont les critères à prendre en compte par la Police grand-ducale pour aviser une telle demande.

Dans cet ordre d'idée, une référence à l'avis de la Cour de Justice de l'Union européenne du 26 juillet 2017 concernant l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers s'avère pertinente. En effet, la Cour a estimé que pour que l'accord envisagé soit compatible avec les articles 7 et 8, ainsi qu'avec l'article 52 paragraphe (1) de la Charte européenne des droits de l'homme, il doit, entre autres, *« prévoir que les modèles et les critères utilisés dans le cadre du traitement automatisé des données PNR seront spécifiques et fiables ainsi que non discriminatoires » et « que les bases de données utilisées seront limitées à celles exploitées par le Canada en rapport avec la lutte contre le terrorisme et la criminalité transnationale grave. »*[315]. Le Contrôleur européen de la protection des données avait noté dans ce contexte qu'une évaluation sur base de critères inconnus en constante évolution suscite d'importantes inquiétudes en matière de transparence et de proportionnalité[316].

Il convient de citer par ailleurs l'article 12 de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, qui énumère, sauf exceptions prévues dans son paragraphe (3), les informations à mettre à disposition de la personne concernée par le responsable du traitement, comme par exemple les finalités du traitement, la base juridique du traitement, la durée de conservation des données ou encore les catégories de destinataires des données

[315] Avis 1/15 de la CJUE du 26 juillet 2017 concernant l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, paragraphe 232.
[316] Avis 2011/C 181/02 du 22 juin 2011 du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, paragraphe 16.

à caractère personnel, ainsi qu'au besoin, des informations complémentaires. Pour les raisons susmentionnées de transparence, la CNPD est d'avis que les demandeurs d'une vérification des antécédents doivent être informés des critères sur lesquels la Police grand-ducale avise leur demande et le ministre prend sa décision.

Dans un souci de transparence et de sécurité juridique, la CNPD recommande d'intégrer les durées de validité des différentes vérifications des antécédents dans le corps du texte du projet de règlement grand-ducal.

3. Les données traitées dans le cadre de l'avis de la Police grand-ducale et de la décision du ministre

La CNPD relève qu'il semble exister une contradiction entre l'article 1er paragraphe (2) du projet de loi n°7475 qui prévoit que le ministre prend les décisions relatives à la vérification des antécédents sur « avis » de la Police grand-ducale, et l'article 13 paragraphe (1), deuxième phrase du projet de règlement grand-ducal qui impose non seulement à la Police grand-ducale la transmission d'un avis au ministre, mais également de *« toutes les données émanant de la recherche des antécédents ».*

Les textes sous avis étant plus que vagues, un certain nombre de questions se posent à cet égard :

- Y a-t-il création d'un nouveau fichier par la Police grand-ducale dans la mesure où celle-ci procède à la collecte directe et indirecte de données dans le cadre des vérifications des antécédents des demandeurs ?

- Le fait-elle à titre de responsable du traitement ou à titre de sous-traitant pour le compte du ministre ? (cf. point *« 1.2. Quant au responsable du traitement »* du présent avis)

- L'avis à émettre par la Police grand-ducale sur base du nouvel article 1er paragraphe (2) du projet de loi n°7475 est-il limité à une appréciation positive ou négative relative à la demande, dans la mesure où l'avis doit a priori être accompagné de toutes les données émanant de la recherche des antécédents ?

- Dans la mesure où l'article 13 paragraphe (1) du projet de règlement grand-ducal prévoit que la Police grand-ducale doit continuer toutes les données émanant de la recherche des antécédents au ministre ayant la Police grand-ducale dans ses attributions, créera-t-il également un fichier dans le cadre du traitement de données en question ou supprimera-t-il les données après sa prise de décision ?

Enfin, l'article 13 paragraphe (1) du projet de règlement grand-ducal prévoit que dans le cadre des décisions relatives à la vérification des antécédents, le ministre peut demander à la Police grand-ducale *« toute information supplémentaire qu'il juge nécessaire. »* Le commentaire des articles ne donne pas plus d'explications à cet égard. Cette formulation étant très vague, la CNPD se demande dans quel mesure le ministre demandera des informations supplémentaires. Pourrait-il estimer que les informations prévues aux paragraphes (2) à (4) de l'article 13

du projet de règlement grand-ducal ne sont pas suffisantes pour évaluer la fiabilité d'un demandeur d'une vérification des antécédents ou pourrait-il estimer que le dossier du demandeur lui transmis par la Police grand-ducale est incomplet ou que la Police grand-ducale n'aurait pas vérifié ou pris en compte toutes les informations nécessaires ?

Afin de répondre aux exigences de prévision et de prévisibilité auxquelles doit répondre un texte légal, la CNPD estime nécessaire que les textes sous avis soient clarifiés par rapport aux questions soulevées ci-avant.

4. La durée de conservation des données

L'article 3 paragraphe (1) lettre e) de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale prévoit que le responsable du traitement peut seulement conserver les données à caractère personnel sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles les données sont traitées.

Ni le projet de loi n°7475, ni le projet de règlement grand-ducal sous examen ne précisent une durée de conservation des données à caractère personnel traitées dans le cadre des demandes de vérification des antécédents.

La CNPD rappelle dans ce contexte que dans son avis du 28 décembre 2017 relatif au projet de loi n°7168 de transposition de la Directive 2016/680[317], la CNPD avait estimé que l'article 5 de la Directive 2016/680 n'était pas correctement transposé en droit national en ce sens qu'il ne devrait pas appartenir à chaque responsable du traitement de fixer les délais de conservation des données, mais qu'il devrait revenir au législateur de les fixer de manière précise dans des lois spéciales et ceci pour chaque traitement de données. Le législateur n'avait cependant pas suivi l'argumentation de la CNPD en choisissant de confier au responsable du traitement la fixation des délais de conservation des données ainsi que les règles procédurales en vue d'assurer le respect de ces délais[318].

Or, dans le contexte des discussions actuelles relatives au fichier central de la Police grand-ducale, le ministre ayant la Police grand-ducale dans ses attributions a informé la Chambre des députés qu'un projet de loi précisant le cadre législatif du fichier central de la Police grand-ducale et, le cas échéant, d'autres fichiers de la Police, et prenant en compte les recommandations de la CNPD, serait soumis à la Chambre des députés avant les vacances de Noël.[319] Dans cette optique, la CNPD estime nécessaire que le projet de loi n°7475 devrait préciser les délais de conservation des données.

D'autres pays ont précisé des durées de conservation spécifiques dans leurs lois nationales, comme par exemple l'Allemagne. En effet, le paragraphe (11) 1er point de la section 7 de la loi allemande précitée concernant la sécurité aérienne prévoit que les administrations de la sûreté du transport aérien sont obligées de supprimer les données collectées dans le cadre de la vérification des antécédents trois ans après la durée de validité de la vérification. En

[317] Délibération n°1049/2017 du 28 décembre 2017.
[318] Article 4 de la loi du 1er août 2018 en matière pénale ainsi qu'en matière de sécurité nationale.
[319] Comme révélé dans un article d'actualité publié le 25 septembre 2019 sur le site de la Chambre des députés : https://cnpd.msp.etat.lu/Docrdp/2018/2019%2009%2026%20CHD%20Chambre%20des%20D%C3%A9put%C3%A9s%20du%20Grand-Duch%C3%A9%20de%20Luxembourg.pdf (consulté en dernier lieu le 5 décembre 2019).

cas de décision négative, la suppression des données s'impose deux ans après le refus ou la révocation et en cas de retrait d'une demande par la personne concernée, immédiatement après ledit retrait au cas où la demande n'a pas encore été traitée. Le point 2 du paragraphe (11) de la section 7 précitée prévoit des durées de conservation spécifiques pour différentes autorités publiques, qui sont limitativement énumérées par la loi en question, et auxquelles les administrations de la sûreté du transport aérien peuvent demander des renseignements, comme par exemple aux autorités répressives. Ces autorités sont obligées de supprimer les données traitées dans le cadre d'une vérification des antécédents trois mois après la fin de validité d'une vérification, calculé à partir du moment de la demande de renseignement par une administration de la sûreté du transport aérien, ou, immédiatement après avoir été informé par une telle administration d'un refus, retrait ou d'une révocation d'une demande de vérification des antécédents.

Ainsi, la CNPD rappelle sa recommandation émise dans le cadre de son avis relatif au fichier central de la Police grand-ducale dans lequel elle estime que *« les délais de conservation ou du moins les critères applicables pour déterminer la durée de conservation ainsi que les procédures permettant la vérification régulière de la nécessité lesdits délais mériteraient d'être précisés par le législateur afin de limiter au maximum la marge de manœuvre du responsable du traitement et garantir la transparence, l'accessibilité et la proportionnalité desdits délais. »*[320].

En conclusion, la CNPD estime qu'en l'état actuel, les textes sous avis ne respectent pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal. Elle estime nécessaire que les textes soient précisés sur les points suivants :

- la détermination du responsable du traitement et de l'éventuel sous-traitant, voire même d'une responsabilité conjointe dans le cadre du traitement des demandes de vérification des antécédents ;

- les finalités poursuivies par le traitement de données ;

- les éventuels accès de la Police grand-ducale à ses propres fichiers, aux autres fichiers nationaux et aux systèmes d'information européens et internationaux dans le cadre des demandes de vérifications des antécédents ;

- les modalités d'accès et d'échange de données entre la Police grand-ducale et le ministre dans ce contexte et l'éventuelle création de nouveaux fichiers ;

- la durée de conservation des données ;

- les critères à prendre en compte par la Police grand-ducale pour aviser une demande de vérification des antécédents ;

[320] Délibération n°45/2019 du 13 septembre 2019, p. 30.

- les critères à prendre en compte par le ministre pour accorder ou refuser une demande de vérification des antécédents ;

- les entités visées à l'article 13 paragraphe (3) point 4° du projet de règlement grand-ducal par les termes « autorités nationales compétentes », ainsi que les conditions et modalités du transfert de données de ces autorités vers la Police grand-ducale ;

- les durées de validité des différentes vérifications des antécédents ;

- les critères à prendre en compte par la Police grand-ducale dans le cadre des autorisations spécifiques accordées, le cas échéant, aux visiteurs et membres de la presse, ainsi que des précisions sur l'autorité compétente pour délivrer des laissez-passer journalier pour les visiteurs et membres de la presse.

Ainsi décidé à Esch-sur-Alzette en date du 17 décembre 2019.

La Commission nationale pour la protection des données

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

ANNEXES

5

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°6961 portant 1. création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2) du Code pénal.

Délibération n°60/2019 du 17 décembre 2019

Conformément à l'article 46, paragraphe 1er, lettre (c) de la directive (UE) n°2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après désignée « la Directive »), à laquelle se réfère l'article 8 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données (ci-après désignée « loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD »), «conseille la Chambre des députés, le Gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données personnelles ».

Par courrier du 18 novembre 2019, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet d'amendements au projet de loi n°6961 portant 1. création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2) du Code pénal.

En date du 16 juillet 2018, la CNPD avait rendu un premier avis au sujet du projet de loi n°6961[321].

Par ailleurs, par un courrier du 8 juin 2016, Monsieur le Premier Ministre avait invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité, règlement à prendre en exécution de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité. La CNPD avait avisé ledit projet de règlement grand-ducal en date du 13 juillet 2016[322].

En 2013, la CNPD avait par ailleurs rendu un avis relatif à un avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.[323]

[321] Délibération n°444/2018 du 16 juillet 2018
https://cnpd.public.lu/fr/decisions-avis/20171/444-pl6961-ANS.html
[322] Délibération n°639/2016 du 13 juillet 2016
https://cnpd.public.lu/fr/decisions-avis/2016/SRE.html
[323] Délibération n°274/2013 du 28 juin 2013
https://cnpd.public.lu/fr/decisions-avis/2013/sre.html

Article 28 paragraphe (1) projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité

L'article 28 paragraphe (1) alinéa 1 lettre i) projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité prévoit que, dans le cadre des enquêtes de sécurité ou des enquêtes de sécurité ultérieures, l'ANS a un accès direct, par un système informatique, à la partie « recherche » de la banque de données nominatives de police générale. Par ailleurs, l'alinéa 2 de l'article 28 paragraphe (1) prévoit que l'ANS peut s'adresser au Procureur général afin d'obtenir des informations provenant de la partie « documentaire » de la banque de données.

Il convient de rappeler que ladite banque de données était jadis régie par le règlement grand-ducal du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale. Ledit règlement est abrogé implicitement depuis l'entrée en application de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données ce qui pose des questions sérieuses quant à la base légale du traitement de données en question[324].

La loi se réfère donc à un traitement de données qui n'est expressément prévu par aucun texte légal et dont certains éléments clés relèvent désormais de la pratique administrative de la Police grand-ducale. Tel est par exemple le cas de la division de la banque de données en une partie « recherche » et une partie « documentaire » auxquelles il est fait référence dans l'article 28 paragraphe (1).

Article 28 paragraphe (5) projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité

L'article 28 paragraphe (5) projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité tel qu'amendé donne à la CNPD la compétence de surveiller l'accès prévu par le paragraphe (1) du même article 28.

La CNPD tient cette même compétence générale de surveillance déjà en vertu de 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.*

Les articles 24 et 28 de la *loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale* prescrivent des fichiers de journalisation en matière d'accès à des données tels que ceux prévus par l'article 28 paragraphe (1) projeté de la loi modifiée du 15 juin 2004. Cependant, afin de garantir un contrôle utile et efficace a posteriori des accès via les fichiers de journalisation, il conviendrait de fixer, dans la loi modifiée du 15 juin

[324] voir à ce sujet l'avis de la CNPD au sujet du fichier central de la Police grand-ducale au regard de la législation en matière de protection des données, délibération n°45/2019 du 13 septembre 2019
https://cnpd.public.lu/fr/decisions-avis/2019/45-fichier-central-police.html

2004, la durée de conservation des fichiers de journalisation à 5 ans, qui correspond par ailleurs à la durée de prescription des délits[325].

Article 29 projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité (Amendement 20)

En matière de durée de conservation, l'amendement remplace la référence 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, référence contenue dans l'article 29 paragraphe (3) projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, par le passage suivant :

« Les données relatives à l'enquête de sécurité sont détruites ou effacées conformément aux dispositions de la loi du 1er août 2018 jj/mm/aaaa relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale :

- *endéans les six mois suivant la décision de refus sauf si les raisons pour lesquelles elles ont été recueillies sont toujours d'actualité ;*

- *endéans les cinq ans après que le candidat ait cessé son activité requérant l'accès à des pièces classifiées. »*

Si la formulation actuelle est certes préférable à la simple référence à la loi contenue dans l'article 29 projeté avant les amendements sous avis, la CNPD se demande cependant ce qu'il faut comprendre précisément par *« raisons pour lesquelles elles ont été recueillies sont toujours d'actualité »*. En effet, si la raison de la collecte des données était une demande d'habilitation, celle-ci n'existe plus puisque le passage en question se rapporte précisément à l'hypothèse d'un refus.

Article 31 projeté de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité (Amendement 21)

L'amendement 20 rajoute aux critères d'appréciation (que l'ANS prend en compte en matière de garanties de discrétion, loyauté, fiabilité et intégrité) les critères suivants :

« n) l'existence d'un ou de plusieurs incidents de sécurité ;

o) le fait d'avoir ou d'avoir eu des comportements de nature à entraîner un risque de vulnérabilité au chantage ou à des pressions ;

[325] Par exemple des infractions prévues par les articles 509-1 et suivants du Code pénal ou celles prévues par l'article 47 paragraphe (3) de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

p) le fait d'avoir fait preuve, en acte ou en parole, d'un manque d'honnêteté, de loyauté ou de fiabilité ou de s'être montré indigne de confiance. ».

La CNPD estime que les libellés sont assez vagues même si elles trouvent leur source en partie dans des textes juridiques européens. Cette imprécision peut être source d'incertitudes et d'insécurité juridique.

Ainsi décidé à Esch-sur-Alzette en date du 17 décembre 2019.

La Commission nationale pour la protection des données

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

ANNEXES

5

NOTES

CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

15, Boulevard du Jazz - L-4370 Belvaux
Téléphone : +352 26 10 60-1 - Fax : +352 26 10 60-6099
www.cnpd.lu