N° 7184[3]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

portant création de la Commission nationale pour la protection des données et la mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat 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

* * *

SOMMAIRE:

*

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(28.12.2017)

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

Faisant suite à la demande lui adressée par Monsieur le Ministre des Communications et des Médias en date du 22 août 2017, la CNPD entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n° 7184 relative à la création de la Commission nationale pour la protection des données et la mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après : « le projet de loi »).

La protection des données à caractère personnel constitue une des dimensions du droit au respect de la vie privée ; elle est désormais consacrée comme un droit fondamental à part entière dans la Charte des droits fondamentaux de l'Union européenne (article 8). Depuis l'avènement de l'ère du numérique, elle revêt une dimension particulière.

La Commission nationale rejoint les auteurs du présent projet de loi, en ce que le cadre législatif actuel relatif à la protection des données qui date de 1995 est dépassé par l'évolution rapide des technologies et la mondialisation qui ont créé de nouveaux enjeux pour la protection des données à caractère personnel, vu l'ampleur de la collecte et du partage de données à caractère personnel qui a augmenté de manière importante.

Il est vrai que ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union européenne, assorti d'une application rigoureuse des règles via des sanctions dissuasives en cas de violation constatée. S'il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur européen, il est également indispensable de renforcer la protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement de leurs données personnelles. En 2012, la Commission européenne a initié une réforme du cadre existant, visant à adapter les règles aux nouveaux défis réglementaires, et ceci en assurant une neutralité technologique dans un souci de pérennité et en tenant compte de l'évolution technologique et sociétale des deux dernières décennies.

Une réforme de la protection des données sous Présidence luxembourgeoise du Conseil de l'Union européenne, a conduit à l'adoption du règlement (UE) 2016/679 (ci-après : « le RGPD »), tenant à harmoniser les règles nationales existantes et à moderniser la directive 1995/46/CE, a pour but de renforcer la protection 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.

En outre, le RGPD uniformise et simplifie les règles auxquelles les organismes traitant des données personnelles sont soumis en renforçant les garanties d'ores et déjà offertes par la directive 95/46 (CE). Il prévoit en particulier la réduction des formalités préalables pour la mise en oeuvre des traitements comportant moins de risques, avec le passage d'un système de contrôle *a priori* par la CNPD, par le biais de notifications et d'autorisations, à un contrôle *a posteriori* plus adapté aux réalités du terrain.

En contrepartie, la CNPD voit ses pouvoirs de contrôle et de sanctions renforcés avec la possibilité d'infliger des amendes pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial de l'organisme concerné.

Un tel changement de paradigme nécessite une évolution des missions et pouvoirs de l'ensemble des autorités de protection des données de l'Union européenne dont la CNPD.

Dans ce nouvel environnement juridique, la CNPD devra notamment guider encore plus les acteurs, notamment les petites et moyennes entreprises qui doivent s'adapter aux nouvelles obligations en matière de protection des données.

Les autorités de contrôle européennes devront également coopérer rapidement dans le cadre du « guichet unique » instauré par le RGPD, un mécanisme de coopération renforcé entre les autorités de protection des données qui devront dorénavant adopter des décisions communes lorsque les traitements de données seront transnationaux, ainsi que pour parvenir à une position commune unique pour toute l'Union européenne au sein du nouveau Comité européen pour la protection des données. Les décisions prises par cet organe constitueront le gage d'une plus grande sécurité juridique pour les responsables de traitement et d'une application uniforme de la législation européenne en matière de protection des données.

Deux autres instruments européens s'ajoutent au RGPD pour constituer le « paquet sur la protection des données », réformant en profondeur le droit de la protection des données au niveau de l'Union européenne. Ainsi, le Parlement européen et le Conseil ont adopté parallèlement en date du 27 avril 2016:

– la directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après : « la directive 2016/680 ») faisant l'objet de l'avis xy de la CNPD du xx décembre 2017 et
– la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) 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 (ci-après : « la directive PNR ») faisant l'objet de l'avis 958 de la CNPD du 23 novembre 2017.

Comme il s'agit en la matière d'un règlement européen qui est d'application directe, c'est le règlement (UE) 2016/679 qui déterminera la majorité des dispositions de fond désormais applicables en matière de protection des données.

Selon les auteurs du projet de loi sous examen, ce dernier, qui doit se lire conjointement avec le règlement (UE) 2016/679, se limite à compléter ce cadre européen par les dispositions nationales qui s'imposent, à savoir :

– la mise en place/l'adaptation de la loi organique de la Commission nationale pour la protection des données (actuellement contenue dans la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel qui devra être abrogée), afin d'octroyer à la CNPD les nouveaux pouvoirs qui lui seront nécessaires pour que celle-ci puisse exercer les missions qui lui sont dévolues par le nouveau règlement (UE) 2016/679 (chapitre 1);
– les dispositions spécifiques dans des domaines où le règlement (UE) 2016/679 prévoit qu'une législation nationale complémentaire peut être adoptée (chapitre 2).

Les auteurs du projet de loi ont fait le choix d'abroger la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. La Commission nationale acquiesce ce choix qui permet une meilleure articulation entre les dispositions prises en exécution du RGPD et celles visant à transposer la directive 2016/680. D'autant plus que les auteurs du projet de loi visant à transposer la directive 2016/680 vont au-delà du champ d'application de la directive pour y intégrer les traitements de données personnelles effectuées en matière de sécurité nationale et de désigner la future CNPD comme successeur de l'autorité de contrôle de l'article 17 de la loi de 2002, actuellement compétente en la matière.

Elle constate que de manière générale, le projet de loi sous avis remplit globalement l'objectif principal qui lui est assigné, à savoir adapter le droit luxembourgeois au nouveau cadre européen pour en assurer la pleine effectivité pour les citoyens et les responsables de traitement et sous-traitants.

Il donne ainsi corps au RGDP, qui constitue une avancée considérable pour la protection des données à caractère personnel dans l'Union européenne.

Sous réserve des clarifications demandées, omissions relevées ou compléments proposés ci-après dans le cadre de l'examen section par section, le projet de loi dote en effet le régulateur des pouvoirs nécessaires à l'exercice de ses missions.

A. Quant à la mise en place d'une nouvelle loi organique pour la CNPD

Le règlement (UE) 2016/679, tenant à harmoniser les règles nationales existantes et à moderniser la directive 1995/46/CE, déterminera la majorité des dispositions de fond désormais applicables en matière de protection des données.

Il se caractérise par la mise en place d'une approche dite de « l'accountability » c'est-à-dire une responsabilisation des acteurs qui traitent des données personnelles, via un autocontrôle des entreprises.

Il s'ensuit que la nouvelle CNPD passera d'un système de contrôle a priori (donc le système des notifications et autorisations tel que prévu actuellement par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel) vers un contrôle a posteriori.

Ce changement de paradigme permettra à la nouvelle CNPD de se concentrer davantage sur sa mission de sensibilisation et de guidance des responsables de traitement de données. Pour que le système soit dissuasif, la nouvelle Commission nationale devra disposer d'une compétence plus large et de moyens de contrôle et de sanction nettement plus conséquents et dissuasifs en cas de violation constatée que ce dont l'actuelle CNPD dispose.

Le présent avis est donné à l'égard du projet de loi 7184, mais pour ce qui concerne la mise en place d'une nouvelle Commission nationale pour la protection des données, ce dernier est indissociable du projet de loi 7168. Il s'ensuit que non seulement le présent avis devra être lu ensemble avec l'avis de la Commission nationale sur le projet de loi 7168 (délibération n° 1049/2017 du 28 décembre 2017), mais le présent avis y référera aussi.

1. *Statut juridique et indépendance*

Malgré son nom, le projet de loi n'entend pas créer une nouvelle autorité de surveillance générale mais plutôt revoir les fondements de l'autorité existante et élargir ses compétences, tout comme ses missions et pouvoirs.

La nécessité de prévoir une telle autorité de contrôle réside dans l'article 16, paragraphe 2 du Traité sur le fonctionnement de l'Union européenne, qui est précisément la base légale du RGPD et de la Directive 2016/680, ainsi que dans l'article 8, paragraphe 3, de la Charte des droits fondamentaux de l'Union européenne, qui prévoient tous les deux que le respect des règles y prévues est soumis au contrôle d'autorités indépendantes.

Tout comme la CNPD actuelle, la nouvelle commission prendra la forme d'un établissement public, seule forme juridique qui permette d'atteindre le but de garantir un niveau d'indépendance certain à la CNPD.

La CNPD dispose ainsi de la personnalité juridique et jouit de l'autonomie financière et administrative nécessaire à garantir son indépendance face à l'exécutif, auquel elle n'est attachée que pour des questions liées aux spécificités de fonctionnement de l'Etat luxembourgeois et aucunement sous une tutelle au sens littéral du terme qui ne lui permettrait pas de prendre librement ses décisions. Autrement comprise, la disposition se heurterait à l'article 52 du RGPD qui dispose que dans l'exercice de leurs missions et de leurs pouvoirs, le ou les membres de chaque autorité de contrôle demeure libre de toute influence extérieure, qu'elle soit directe ou indirecte et ne sollicitent ne n'acceptent d'instructions de quiconque. L'article 4 du projet de loi reprend d'ailleurs à juste titre cette disposition.

Il importe également que la CNPD dispose d'un budget annuel qui lui permette de remplir ses missions tout comme le prévoit le RGPD dans le paragraphe 4 de l'article 52 : « Chaque Etat membre veille à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsque celle-ci doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au Comité. » Il est de la volonté du législateur européen que le budget des autorités de contrôle soit pris en charge par l'Etat directement et non que l'autorité de contrôle couvre l'entièreté de ses frais de fonctionnement par des redevances qu'elle serait autorisée à percevoir.

La Commission nationale salue l'introduction d'un nouveau pouvoir par rapport à la loi de 2002, à savoir la possibilité d'adopter des règlements CNPD dans la limite de sa spécialité. Cette disposition permettra à la nouvelle Commission nationale de réagir rapidement aux développements sur le terrain pour mieux guider les acteurs et si nécessaire de spécifier certaines règles dans un objectif d'augmenter la sécurité juridique.

2. *Compétences de la CNPD*

A l'heure actuelle, la loi du 2 août 2002 sur la protection des personnes à l'égard du traitement des données à caractère personnel institue en son article 32 (1) une autorité de contrôle dénommée « Commission nationale pour la protection des données » chargée de contrôler et de vérifier si les données soumises à un traitement sont traitées en conformité avec les dispositions de cette loi et ses règlements d'exécution. Cette autorité de contrôle a une compétence générale de supervision en matière de protection des données. On peut considérer qu'elle est l'autorité de contrôle de droit commun pour ce qu'on peut appeler le « régime général » de la protection des données à caractère personnel, en ce sens qu'elle est compétente pour toute la matière, sauf disposition légale contraire.

La loi de 2002 prévoit une autorité de contrôle spécifique composée du Procureur Général d'Etat, ou de son délégué et de deux membres de la Commission nationale, communément appelée « Autorité de contrôle Article 17 » d'après l'article qui l'institut. Cette autorité de contrôle spécifique est exclusivement compétente pour surveiller les traitements de données visés à l'article 17 de ladite loi (p.ex. traitements effectués par la Police grand-ducale, le Service de renseignement de l'Etat, l'Administration des Douanes et Accises etc.).

Une nouveauté majeure apportée par le projet de loi est l'élargissement des compétences de la CNPD à des traitements des données à caractère personnel en matière pénale et de sécurité nationale. La nouvelle Commission nationale aura donc également compétence pour des matières revenant actuellement de l'autorité de contrôle de l'article 17, qui disparaîtra toutefois avec l'abrogation de la loi de 2002 prévue par le projet de loi sous avis. La nouvelle Commission nationale sera dès lors la seule

autorité de contrôle pour les traitements de données personnelles généraux tant sous le RGPD que le projet de loi de la Directive 2016/680 et le garant pour une application correcte de ces deux instruments ainsi que de tous les textes normatifs se rapportant à la protection des données, ce qui permettra d'assurer une mise en oeuvre et une interprétation cohérente des règles en matière de protection des données.

Tant le RGPD que la Directive prévoient que les données à caractère personnel traitées par les juridictions dans l'exercice de leur fonctions juridictionnelles sont exclues de la surveillance des autorités de contrôle.

L'article 55 paragraphe 3 du RGPD laisse présumer que lesdits traitement pourraient être exempts de contrôle. Ce n'est toutefois pas la voie choisie par le législateur luxembourgeois qui préconise la création d'une nouvelle autorité de contrôle séparée, aux termes de l'article 41 du projet de loi N° 7168. Cette autorité de contrôle judiciaire sera compétente pour la supervision des traitements effectuées par les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif dans l'exercice de leurs fonctions juridictionnelles, que ce soit pour les finalités prévues par l'article 1 dudit projet de loi 7168 ou pour celles visées par le RGPD. Ces traitements sont donc exclus de la compétence de la nouvelle Commission nationale.

L'article 8 du projet de la loi prévoit que c'est la Commission nationale qui représente le Luxembourg au « Comité européen de la protection des données » institué par l'article 68 de RGPD et contribue à ses activités. C'est une disposition très claire, permettant d'éviter la confusion quant à la question de savoir quelle autorité de contrôle siègera au Comité européen, alors que ce dernier est non seulement compétant pour l'application du RGPD, mais dispose également de certains pouvoirs dans le cadre de la Directive 2016/680.

3. *Missions de la CNPD*

La nouvelle Commission nationale voit ses missions élargies par rapport à celles actuellement prévues. Elle se verra attribuer de nouvelles missions en vertu de la loi de transposition de la directive 2016/680.

a) *Dans le cadre du règlement 2016/679*

C'est l'article 57 du RGPD qui énumère les missions de droit commun de la Commission nationale. Elles ne sont pas reprises expressément dans le projet de loi sous avis, l'article 9 se limitant à se référer au prédit article 57 du RGPD.

b) *Dans le cadre du projet de loi de transposition de la Directive 2016/680*

La liste de missions de la nouvelle Commission nationale reprise dans l'article 10 du projet de loi concerne exclusivement les traitements visés par la Directive 2016/680 qui nécessite une transposition dans le droit national.

Il s'agit d'une copie conforme aux missions prévues aux articles 46 et 48 de la directive 2016/680, ce qui n'appelle pas de remarques particulières en soi. L'article 43 du projet de loi 7168 prévoit exactement la même liste de missions pour l'autorité de contrôle judiciaire.

Les deux autorités de contrôle devront non seulement veiller à ne pas empiéter sur le champ de compétence de l'une et de l'autre, mais également se concerter dans un souci d'harmonisation dans l'application et l'interprétation des textes législatifs nationaux, européens et internationaux en matière de protection des données. Les auteurs du projet de loi 7168 ont toutefois déjà devancé le risque de disparité de jurisprudence en prévoyant qu'un membre de la CNPD fasse partie de l'autorité de contrôle judiciaire.

4. *Les pouvoirs de la CNPD*

« Afin de veiller à faire appliquer le RGPD et à contrôler son application de manière cohérente dans l'ensemble de l'Union, les autorités de contrôle devraient avoir dans chaque Etat membre les mêmes pouvoirs effectifs… » prévoit le considérant (129) du RGPD. L'article 58 paragraphes 1, 2 et 3

du RGPD qui énumère ces pouvoirs obligatoires pour chaque État membre. Ces derniers ne peuvent que rajouter des pouvoirs additionnels, ce que les auteurs du projet de loi sous avis ne font pas, mais pas en retirer.

Par contre, chaque État membre doit en vertu de l'article 58 paragraphe 5 du RGPD prévoir, par la loi, que son *« autorité de contrôle a le pouvoir de porter toute violation du RGPD à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement. »* C'est un article qui impose une action aux États membres en laissant à leur appréciation les moyens déployés pour atteindre le résultat escompté.

Alors que l'article 15 du projet de loi sous avis se borne à indiquer le principe que la CNPD a le droit d'ester en justice, les auteurs du projet de loi restent muets sur la procédure judiciaire à suivre.

Le projet de loi ne précise rien non plus sur l'obligation de prévoir dans le droit national le pouvoir de la nouvelle CNPD de porter toute violation du RGPD à l'attention des autorités judiciaires.

Comme le spectre des infractions pénales a presque été réduit à néant dans les deux projets de lois, la CNPD ne pourra porter une violation du RGPD à l'attention des autorités judiciaires, par le biais d'une dénonciation au parquet, que dans cinq cas, dans la mesure où le projet de loi sous avis prévoit une seule infraction pénale et le projet de loi N° 7186 en prévoit quatre : La possibilité de saisir les autorités judiciaires de violations du RGPD par ce biais est donc presque inexistante. La question de savoir s'il ne serait pas judicieux de prévoir des sanctions pénales pour des violations intentionnelles du RGPD sera traitée dans la section relative aux sanctions.

Il n'en reste pas moins qu'en vertu de l'article 58 paragraphe 5 du RGPD, la CNPD doit avoir la possibilité de porter toute violation du RGPD à l'attention des autorités judiciaires et notamment aussi des violations commises par les institutions européennes.

Etant donné que la Commission nationale dispose de la personnalité juridique, il va de soi qu'elle peut ester en justice pour défendre ces décisions dans le cadre de l'article 54 du projet de loi sous avis. Or, quelle procédure judiciaire peut-elle emprunter pour faire appliquer les dispositions du présent règlement, notamment pour faire analyser la validité de certaines décisions prises par les institutions européennes sur base du RGPD par la Cour de justice de l'Union européenne?

Dans ce contexte, il convient par ailleurs de rappeler et de souligner l'importance de l'obligation faite aux Etat membres dans l'arrêt « Schrems » du 6 octobre 2015 rendu par la CJUE (affaire C-362/14).

Les juges retiennent au point 65 de l'arrêt que *« Dans l'hypothèse contraire, où ladite autorité estime fondés les griefs avancés par la personne l'ayant saisie d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de ses données à caractère personnel, cette même autorité doit, conformément à l'article 28, paragraphe 3, premier alinéa, troisième tiret, de la directive 95/46, lu à la lumière notamment de l'article 8, paragraphe 3, de la Charte, pouvoir ester en justice. À cet égard,* ***il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision*** *»*

La décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis reprend à son compte la décision de la CJUE dans son point 144 :

> *« La Cour de justice a par ailleurs considéré que, conformément à l'article 25, paragraphe 6, second alinéa, de la directive 95/46/CE, les États membres et leurs organes doivent prendre les mesures nécessaires pour se conformer aux actes des institutions de l'Union, car ces derniers jouissent, en principe, d'une présomption de légalité et produisent, dès lors, des effets juridiques aussi longtemps qu'ils n'ont pas été retirés, annulés dans le cadre d'un recours en annulation ou déclarés invalides à la suite d'un renvoi préjudiciel ou d'une exception d'illégalité. En conséquence, une décision d'adéquation de la Commission adoptée conformément à l'article 25, paragraphe 6, de la directive 95/46/CE a un caractère contraignant pour tous les organes des États membres destinataires, y compris leurs autorités de surveillance indépendantes . Lorsqu'une telle autorité a été saisie d'une plainte concernant la compatibilité d'une décision d'adéquation de la Commission avec la protection des droits fondamentaux que constituent le respect de la vie privée et la protection*

des données et qu'elle estime que les griefs avancés sont fondés, le droit national doit prévoir des voies de recours lui permettant de faire valoir ces griefs devant les juridictions nationales, qui, en cas de doute, doivent surseoir à statuer et procéder à un renvoi préjudiciel devant la Cour de justice. »

Le droit national actuel n'est donc pas conforme à la jurisprudence de la CJUE, alors qu'il ne prévoit actuellement pas de voie de recours ou de procédure judiciaire permettant à la CNPD de saisir directement une juridiction nationale dans le cas de figure visé ci-avant. Ce n'est qu'à l'occasion d'un recours devant les juridictions administratives, intenté par une personne concernée ou un responsable de traitement, contre une décision administrative prise par la CNPD, qu'un renvoi préjudiciel devant la CJUE peut être demandé. Or, ceci n'est pas suffisant au regard de l'arrêt précité, alors que les juges européens exigent clairement la possibilité d'une saisine directe des juridictions nationales par l'autorité de contrôle, c'est-à-dire la CNPD.

Le projet de loi sous avis ne comble pas cette lacune et ne lève pas cette non-conformité, de sorte que la CNPD doit insister à ce que le projet de loi soit complété et précisé sur ce point.

Ainsi, il y a lieu de prévoir une disposition dans le projet de loi qui permette à la nouvelle Commission nationale de demander au Tribunal administratif d'ordonner la suspension ou la cessation du transfert de données, dans le cas où, saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, elle estime fondés les griefs avancés, dans l'attente de l'appréciation par la Cour de Justice de la validité d'une décision d'adéquation de la commission européenne prise sur le fondement du RGPD ou des articles de la Directive ou de tout acte pris par la Commission européenne autorisant ou approuvant les garanties appropriés pris sur le fondement du RGPD ou des articles de la Directive.

Cette saisine devra également être possible tant dans le cadre d'une réclamation dirigée contre un responsable de traitement ou d'un sous-traitant, qu'en dehors d'une telle réclamation, afin que la nouvelle CNPD puisse également agir lorsqu'elle estime que la décision européenne permettant le transfert n'est pas valide.

La teneur d'une disposition pour la nouvelle loi luxembourgeoise sur la protection des données personnelles pourrait être la suivante :

Demande de contrôle juridictionnel par l'autorité de contrôle en cas de présomption d'illégalité d'une décision de la Commission Européenne

(1) Dans le cas où, saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, la Commission nationale pour la protection des données estime fondés les griefs avancés relatifs à la protection des droits d'une personne à l'égard du traitement de ses données à caractère personnel, ou de manière générale afin d'assurer la protection de ces droits dans le cadre de sa mission, peut demander au Tribunal administratif d'ordonner la suspension ou la cessation d'un transfert de données en cause, le cas échéant, sous astreinte, et assortit alors ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de la décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE) 2016/679 ainsi que de tous les actes pris par la Commission européenne autorisant ou approuvant les garanties appropriées dans le cadre des transferts de données pris sur le fondement de l'article 46 de même règlement.

(2) Lorsque le transfert de données en cause ne constitue pas une opération de traitement effectuée par une juridiction dans l'exercice de sa fonction juridictionnelle ou le Ministère public, la Commission nationale pour la protection des données peut saisir dans les mêmes conditions le Tribunal administratif pour obtenir la suspension du transfert de données fondé sur une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de la directive (UE) 2016/680 dans l'attente de l'appréciation par la Cour de justice de l'Union européenne de la validité de cette décision d'adéquation.

(3) Si la Commission nationale pour la protection des données estime qu'une décision d'adéquation de la Commission européenne, prise sur le fondement de l'article 45 du règlement (UE) 2016/679 ainsi que de tous les actes pris par la Commission européenne autorisant ou approuvant les garanties appropriées dans le cadre des transferts de données pris sur le fondement de l'article 46 de même règlement ou règles de conduite approuvées sur fondement de l'article 40 de ce même règlement ou une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de la directive (UE) 2016/680, dont la validité est nécessaire pour

une décision de l'autorité de contrôle, est invalide, elle suspend la procédure et demande un contrôle juridictionnel devant le Tribunal administratif.

(4) La loi du 21 juin 1999 portant règlement de procédure devant les juridictions administratives s'applique conformément au paragraphe (5).

(5) Dans la procédure visée aux paragraphes (1) à (4), la Commission nationale pour la protection des données agit en qualité de demandeur. Le tribunal administratif peut mettre la Cour de justice en mesure de présenter ses observations endéans un délai qu'il impartit.

(6) Si un recours sur le contrôle de validité d'une décision de la Commission européenne visée aux paragraphes (1) à (4) est pendante devant la Cour de Justice de l'Union européenne, le tribunal administratif peut ordonner la suspension de l'affaire jusqu'à ce que la Cour de Justice de l'Union européenne ait rendue sa décision.

(7) Si, à l'issue d'un recours visé aux paragraphes (1) à (4), le tribunal administratif parvient à la conviction que la décision de la Commission européenne est valide, il le constate dans sa décision. Autrement, il soumet la question sur la validité de la décision conformément à l'article 267 du Traité sur le Fonctionnement de l'Union Européenne à la Cour de Justice de l'Union européenne pour décision.

L'article 16 du projet de loi énumère un nombre de pouvoirs de la CNPD dans le cadre des missions de l'article 10 du projet sous examen. Transposition littérale de l'article y afférent, à savoir de l'article 47 de la directive 2016/680, les pouvoirs de la nouvelle CNPD dans ce contexte diffèrent de ceux prévus à l'article 58 du RGPD, qui prend le soin de prévoir plus en détail les pouvoirs d'enquête de l'autorité de contrôle. Afin d'aligner les pouvoirs d'enquête de la CNPD dans le contexte du contrôle des traitements de données en matière pénale ainsi qu'en matière de sécurité nationale sur ceux exercés dans le cadre du RGPD, la Commission nationale estime notamment que *« le pouvoir d'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… »* tel que prévu à l'article 58 paragraphe 1 lettre f) du RGPD devrait aussi être prévu explicitement pour éviter qu'un responsable de traitement ou sous-traitant refuse l'accès à la nouvelle CNPD au motif qu'elle ne disposerait pas de ce pouvoir. Il est peu concevable que la nouvelle Commission nationale puisse exercer son pouvoir d'accès à toutes les données à caractère personnel qui sont traitées et à toutes les informations nécessaires à l'exercice de ses missions si elle n'a pas explicitement le pouvoir d'accès aux locaux. Etant donné que ce pouvoir est prévu textuellement dans le RGPD, il peut difficilement être contenu implicitement parmi les pouvoirs de la Commission nationale dans le cadre du projet de loi de transposition de la Directive.

5. *Certification*

En matière de certification, le RDPD laisse le soin aux Etats membres de décider quelle entité devra « agréer les certificateurs ». Sous le RGPD cela peut être soit l'autorité de contrôle, soit un organisme national d'accréditation, voir les deux. Entre l'ILNAS, l'organisme national de standardisation et la CNPD, le législateur propose de donner cette compétence à la Commission nationale.

La Commission nationale accueille favorablement le choix de la désigner comme organisme national compétent pour délivrer les agréments aux organismes de certification visés à l'article 43, paragraphe 1, du règlement (UE) 2016/679.

Non seulement, la CNPD dispose des connaissances nécessaires spécifiques pour pouvoir assurer cette mission, mais la désignation de l'organisme national d'accréditation désigné conformément au règlement (CE) no 765/2008 (ce qui aurait constitué le choix alternatif) comme organisme national compétent pour sa part, aurait limité la marge de manoeuvre pour la mise en place de schémas de certifications adaptés aux besoins de la place. En effet, en application de l'article 43, paragraphe 3, du règlement (UE) 2016/679, le fait de désigner compétent l'organisme national d'accréditation limiterait un agrément aux organismes de certification qui sont conformes à la norme EN-ISO/IEC 17065/2012 (i.e. norme pour laquelle l'organisme national d'accréditation est compétent). Or, d'autres référentiels, qui sortent du domaine de compétence de l'organisme national d'accréditation, bien établis sur la place et offrant un niveau de qualité similaire existent (p.ex. la norme internationale ISAE 3000 « Missions d'assurance autres que les missions d'audit ou d'examen d'informations financières historiques »).

La CNPD estime par ailleurs que le choix qui a été fait ne l'empêche pas de faire appel aux compétences de l'organisme national d'accréditation luxembourgeois ou d'un autre État membre. En effet,

l'article 43 paragraphe 3, du règlement (UE) 2016/679 laisse à l'autorité de contrôle l'appréciation des critères sur base desquels l'agrément est pris. Ainsi, il est tout à fait possible de retenir pour un schéma de certification donné, comme un critère d'agrément, l'accréditation par un organisme national d'accréditation.

6. *Composition et nomination de la CNPD*

Afin de pouvoir gérer les compétences élargies de la nouvelle Commission nationale, celle-ci est dirigée par un organe collégial composé de quatre membres, soit un de plus qu'actuellement.

Les membres du collège sont autorisés à porter le titre de « Commissaire ». Cette nouveauté ne change rien à la situation des membres du collège au Luxembourg, mais elle apporte une clarification dans le cadre de la coopération européenne. Le terme de « commissaire » est définitivement plus compréhensible à l'étranger que celui de « membre effectif », seul titre que les membres effectifs de la Commission nationale ont jusqu'à présent pu porter sans risque de se rendre coupable d'un abus de titre. Par ailleurs, le terme de « Commissaire » est celui communément utilisé dans les pays francophones pour désigner un membre d'une Commission.

Les Commissaires et membres suppléants sont nommés pour un terme de six ans, renouvelable une fois, ce qui constitue un changement par rapport à la loi de 2002 qui en son article 34 ne prévoyait pas de limitation des mandats. Le RGPD en son article 54 paragraphe 1 e) dispose que *« le caractère renouvelable ou non du mandat du ou des membres de chaque autorité de contrôle et, si c'est le cas, le nombre des mandats »* doit être prévu dans une loi nationale. Le principe de la limitation de mandats est très peu répandu parmi les institutions luxembourgeoises et certains États membres qui ont déjà adopté une nouvelle loi organique pour leurs autorités de surveillance, comme l'Autriche[1] se sont bornés à prévoir le caractère renouvelable du mandat de leur(s) commissaires, sans spécifier le nombre de mandats. La question se pose si le RGPD n'admet pas une interprétation plus large que celle que les auteurs du projet de loi luxembourgeois en font et prévoir un mandat renouvelable sans précision du nombre de mandats.

Tandis qu'aujourd'hui la Commission nationale devra comporter au moins un juriste et un informaticien, le profil combiné des membres du Collège devra à l'avenir être tel que soit assurée au sein du collège une expérience professionnelle solide à la fois en matière juridique, en technologies de l'information et des communications, en matière de protection des données et dans le domaine de la prévention, la recherche, la constatation et la poursuite des infractions pénales.

C'est une approche innovante, qui compte tenu de difficultés de cerner des profils spécifiques, indispensables dans une matière aussi complexe que la protection des données, pour des tâches encore peu connues, ne peut-être qu'accueillie favorablement.

7. *Les agents de la CNPD*

L'article 52 paragraphe 4 du RGPD prévoit que chaque État membre veille à ce que chaque autorité de contrôle dispose des ressources humaines nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsque celle-ci doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité.

Afin de garantir l'indépendance des autorités de contrôle, le RGPD prévoit que ces dernières doivent elle-même choisir et disposer de ses propres agents, qui sont placés sous les ordres exclusifs du ou des membres de l'autorité de contrôle concernée.

L'article 31 apporte une ouverture par rapport aux possibilités de recrutement très rigides prévues par la loi de 2002. À l'avenir la CNPD pourra puiser dans toutes les carrières de l'Etat pour satisfaire ses besoins qui vont au-delà de juristes, d'informaticiens et de rédacteurs.

La question de savoir si la CNPD devrait se doter d'officiers de police judiciaire pour exécuter ses missions d'investigation et d'enquête a été longuement débattue et finalement écartée lorsqu'il se cristallisait que d'un côté, tant le présent projet de loi, que le projet de loi de transposition de la Directive ne comporteraient que très peu de sanctions pénales et que d'autre côté, conférer le statut d'officier de police judiciaire aux agents de la nouvelle CNPD pose un problème par rapport aux exigences d'indé-

---

1 § 20 du Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)

pendance des autorités de contrôle nationales alors que les officiers de police judiciaire seraient sous à la direction du Parquet et que tous les officiers de police judiciaire sont soumis à la surveillance du procureur général.

8. *Fonctionnement de la CNPD*

La nouvelle CNPD établira son règlement d'ordre intérieur dans le mois de son installation. Le règlement d'ordre interne doit être pris à l'unanimité des membres du collège réuni au complet c'est-à-dire au nombre de quatre.

Elle devra se doter de règles procédurales claires, définir son fonctionnement et prévoir l'organisation de ses services. Ce qui est nouveau par rapport à la loi de 2002, c'est que la nouvelle CNPD doit également déterminer les modalités de convocation de membres et de la tenue des réunions collégiales, dispositions qui étaient auparavant prévues par la loi, ce qui pourtant limitait le Collège dans son organisation. Partant, la Commission nationale accueille favorablement la nouvelle flexibilité à ce sujet.

L'adoption du règlement d'ordre intérieur sera certainement une des décisions qui sera prise par les quatre membres du Collège au complet alors que l'article 36 du projet de loi dispose que le Collège ne peut valablement siéger, ni délibérer qu'à condition de réunir trois membres du collège au moins. Pour les cas où le Collège prendrait des décisions au grand complet, il serait toutefois judicieux de prévoir que la voix du président est prépondérante, ce qui permettrait d'éviter une situation de blocage en cas d'égalité des voix.

Etant donné que beaucoup de décisions qui devront être prises par la nouvelle CNPD seront des décisions d'ouverture et de clôture d'enquête et des décisions relatives à des sanctions dans ce cadre, décisions pour lesquelles le Collège ne peut que siéger en formation restreinte pour préserver le principe de la séparation des pouvoirs, il est judicieux de prévoir que trois membres puissent délibérer valablement alors que le chef d'enquête ne peut pas siéger.

Pour les dossiers ayant trait aux enquêtes, il n'y aura que trois commissaires qui pourront valablement siéger, ce qui permettra également de dégager une majorité des voix en cas de décision. Lorsqu'un ou plusieurs membres effectifs non chef d'enquête sera ou seront empêché(s) pour des raisons personnelles ou de conflit d'intérêt, il(s) pourra ou pourront être remplacés par les membres suppléants.

9. *Enquête et décision sur l'issue de l'enquête*

Afin de veiller à l'application du RGPD et à contrôler son application de manière cohérente dans l'ensemble de l'Union européenne, les autorités de contrôle devraient avoir, dans chaque État membre, les mêmes missions et les mêmes pouvoirs effectifs, y compris de pouvoirs d'enquête. C'est l'article 58 du RGPD qui confère ces pouvoirs aux autorités de contrôle, en s'appuyant en partie sur l'article 28, paragraphe 3, de la directive 95/46/CE.

Les auteurs du projet de loi restent sommaires dans l'énoncé des dispositions concernant un domaine qui à l'avenir, avec la disparition des formalités préalables constituera un pilier substantiel du travail de la future Commission nationale. Afin de garantir la prévisibilité du droit applicable, il est indispensable que le Collège de la future Commission nationale adopte un règlement relatif à la procédure applicable aux enquêtes conformément à l'article 5 du projet de loi.

Le projet de loi tend toutefois à régler une question essentielle de procédure liée aux enquêtes, à savoir celle de la séparation des fonctions d'enquête de celles de sanction au sein d'une même entité afin de satisfaire aux critères de l'article 6 § 1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ainsi qu'aux principes d'indépendance et d'impartialité et la nécessité de démontrer une apparence objective de la structure interne de l'autorité de régulation nationale.

Ainsi, le commissaire ayant ordonné l'enquête, ne pourra pas siéger, ni délibérer lorsque le collège décide sur l'issue de l'enquête. Le président pour sa part ne pourra jamais être nommé chef d'enquête.

10. *Dispositions financières*

La Commission nationale pour la protection des données est une autorité de contrôle indépendante, qui en vertu du paragraphe 4 de l'article 52 du RGPD cité ci-avant, se voit doter par l'Etat des ressources financières nécessaires à l'exercice effectif de ses missions et de ses pouvoirs.

L'article 52 paragraphe 4 précité prévoit que les autorités de contrôle doivent également disposer des ressources humaines et techniques, ainsi que des locaux et de l'infrastructure nécessaires. Etant donné que le projet de loi est muet à ce sujet, il y a lieu de constater que la dotation financière de l'Etat doit être suffisante pour couvrir tous les besoins de la nouvelle Commission nationale.

Il est de la volonté du législateur européen que ce soit l'Etat qui couvre les besoins de l'autorité de contrôle bien qu'il ouvre la possibilité à ces dernières de percevoir des redevances dans le cadre de ses pouvoirs d'autorisation et de consultation en vertu de l'article 58, paragraphe 3, du RGPD. Bien évidemment, ces redevances ne peuvent pas être perçues auprès de la personne concernée et, le cas échéant, du délégué à la protection des données dans le cadre de ses missions, alors que pour eux, l'accomplissement des missions des autorités de contrôles est gratuit. Le projet de loi sous avis dans son article 13 rappelle ce principe de gratuité introduit par l'article 57 paragraphe 3 du RGPD. Par contre, rien empêche de percevoir des redevances de la part des responsables de traitements et sous-traitants, pourvu que le montant des redevances soit prévisible. Un règlement de la CNPD devra par conséquent les prévoir.

La vocation de la CNPD n'étant toutefois pas commerciale et son activité n'étant pas commerciale et ne pouvant pas être comparée à une activité commerciale, les redevances ne sont pas destinées à financer la CNPD. Bien que le coût de revient peut-être un élément dans la détermination du montant, il ne doit pas nécessairement l'être.

Il en est différent des paiements que la CNPD peut réclamer en vertu de l'article 13 du projet de loi lorsqu'une demande est manifestement infondée ou excessive. La CNPD peut alors exiger le paiement de frais raisonnables basés sur ses coûts administratifs ou refuser de donner suite à la demande.

Il peut y avoir d'autres cas, comme par exemple dans le cadre de la coopération avec des partenaires pour l'exécution de projets communs, que la CNPD pourra être amenée à percevoir des fonds pour lesquels elle devra tenir une comptabilité. Cette situation est couverte par l'article 48 paragraphe 2 du projet de loi.

11. *Sanctions*

a) *Amendes administratives*

Une des nouveautés du RGPD consiste dans la flexibilité laissée aux responsables de traitement et sous-traitants à organiser eux-mêmes leur conformité au nouveau règlement. En contrepartie de cette flexibilité, toute violation aux dispositions de ce règlement peut entraîner des sanctions administratives financières qui sont « effectives, proportionnées et dissuasives ». Le RGPD confère en effet à la CNPD une nouveau pouvoir de sanction, à savoir d'imposer des amendes administratives.

Vu la spécificité des décisions prises par la CNPD, la Commission nationale conseille de régler toute la procédure liée à l'exécution de ces décisions, dont notamment pour ce qui est des astreintes, dans le présent projet de loi à l'instar de la loi du 23 octobre 2011 relative à la concurrence au lieu de se référer aux articles 2059 à 2066 du Code civil.

Pour ce qui est du recouvrement des amendes administratives et astreintes, l'article 51 du projet de loi donne compétence à l'Administration de l'Enregistrement et des Domaines pour ce qui est des sanctions prononcées à l'égard des personnes physiques et morales de droit privé. La Commission nationale se pose la question de savoir quelle procédure s'applique au recouvrement des amendes administratives et astreintes prononcées à l'égard des personnes morales de droit public, pourtant bel et bien visées par l'article 49 du projet de loi.

b) *Sanctions pénales*

Sous le régime actuel de la loi modifiée du 2 août 2002, les violations des règles en matière de protection des données peuvent surtout être sanctionnées pénalement, la CNPD ne disposant que du pouvoir d'imposer des sanctions administratives, mais non financières.

La loi de 2002 contient en effet pas moins de dix-huit infractions pénales, qui constituent toutes des infractions sui generis et ne figurent pas dans le Code pénal. Le projet loi sous examen se propose d'abroger toutes ces infractions pénales et se limite à n'en conserver qu'une seule, à savoir le délit d'entrave à l'accomplissement des missions de la CNPD, prévu à l'article 53 du projet de loi.

Compte tenu de l'importance des amendes administratives que la CNPD pourra, à l'avenir, imposer en cas de violation du RGPD, nous pouvons entièrement souscrire au choix des auteurs du projet de loi de réduire au maximum les infractions pénales.

Toutefois, il importe de relever que les amendes administratives prévues à l'article 83 du RGPD, peuvent seulement être infligées à l'égard d'un responsable du traitement ou d'un sous-traitant, c'est-à-dire à l'égard de personnes morales privées ou publiques, sauf dans les très rares cas où le responsable du traitement ou le sous-traitant serait une personne physique qui exerce son commerce en nom personnel.

Force est donc de constater que le système des sanctions repose uniquement sur une logique de faire supporter toute la charge des sanctions par les responsables du traitement ou sous-traitants personnes morales, tandis que les personnes physiques qui violent délibérément le RGPD profitent d'une impunité.

Il est vrai que pratiquement toutes les obligations en matière de protection des personnes reposent sur les responsables de traitements ou sous-traitants et qu'il leur incombe de mettre en oeuvre toutes les mesures techniques et organisationnelles nécessaires pour garantir la sécurité et la confidentialité des données. Toujours est-il que même si toutes les mesures imaginables et conformes à l'état de l'art, sont prises, un responsable du traitement ou sous-traitant ne pourra jamais éviter ou exclure que des individus malintentionnés font un usage abusif des données auxquelles ils ont accès dans le cadre de leurs activités.

L'expérience acquise par la CNPD, après quinze ans d'existence, montre que ces cas d'abus de données par des personnes physiques ne sont pas rares, eu égard au nombre important de plaintes de ce genre dont la CNPD a été saisie.

Ainsi p.ex. lorsqu'un salarié ou un agent public utilise abusivement des données auxquelles il a accès dans le cadre de son travail à des fins privées et dans l'intention de nuire à un tiers, la CNPD pourra constater qu'il y a eu violation du RGPD et imposer une amende administrative à l'employeur, responsable du traitement des données ; or, le salarié ne pourra pas faire l'objet de sanction, à l'exception de sanctions disciplinaires infligées par l'employeur.

Ceci n'est bien entendu pas satisfaisant pour une victime d'un usage abusif de ses données qui aura subi un dommage matériel ou moral et qui aura le sentiment que l'Etat accepte que les agissements de l'auteur des faits restent impunis, alors que l'auteur ne pourra pas être poursuivi pénalement. La victime ne pourra pas faire valoir ses droits elle-même, à moins qu'elle n'engage une action judiciaire en matière civile coûteuse.

L'article 84 paragraphe 1 du RGPD prévoit que « Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en oeuvre. Ces sanctions sont effectives, proportionnées et dissuasives. » Le considérant (149) y afférent énonce à ce titre que *« Les États membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violation du présent règlement, y compris de violation des dispositions nationales adoptées en application et dans les limites du présent règlement. Ces sanctions pénales peuvent aussi permettre la saisie des profits réalisés en violation du présent règlement. Toutefois, l'application de sanctions pénales en cas de violation de ces dispositions nationales et l'application de sanctions administratives ne devrait pas entraîner la violation du principe ne bis in idem tel qu'il a été interprété par la Cour de justice »*

La dualité du régime de sanction des violations du RGPD peut donc être prévu par les États membres et tant l'Autriche, que l'Allemagne font usage de cette possibilité dans leurs lois d'adaptation respectives, tout comme la France dans son projet de loi d'adaptation, par lequel elle n'abroge pas les sanctions pénales existantes, et comme la Belgique a l'intention de le faire dans son projet de loi portant exécution du RGPD.

Partant, afin de ne pas laisser impunis des agissements illicites perpétrés par des personnes physiques, que ce soit dans le cadre de traitements de données visées par le présent projet de loi ou du projet de loi 7168, la Commission nationale estime indispensable que le projet de loi érige en infraction pénale :

– le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite ou par des manoeuvres trompeuses,
– le fait de vendre les données à caractère personnel obtenues par les moyens précités et

– le fait, par une personne qui a recueillie, à l'occasion de l'enregistrement, du classement, de la transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir (c'est-à-dire un détournement de finalité).

Dans le cas où il serait tenu compte des suggestions de la CNPD, l'infraction nouvellement créée devrait être ajoutée à l'article 49 du projet de loi 7168.

c) *L'action en cessation*

L'article 52 du projet de loi prévoit l'action en cessation qui est actuellement déjà prévue à l'article 39 de la loi modifiée du 2 août 2002. La CNPD salue les modifications et ajustements apportés par les auteurs du projet de loi à cette procédure, alors qu'elle aura désormais la possibilité de porter une requête devant le président du tribunal d'arrondissement de Luxembourg-Ville sans devoir attendre l'expiration du délai d'un recours ou la confirmation de sa décision par une juridiction. En effet, en raison de l'attente d'expiration des prédits délais, la procédure actuelle de l'action en cessation peut, le cas échéant, seulement être entamée par la CNPD après un délai d'attente de deux à trois ans. Ceci est peu effectif pour une action qui est censée être jugée comme en matière de référé.

Les auteurs du projet de loi énoncent dans le commentaire de l'article 52 que l'action y prévue permettra à la CNPD de faire assurer l'exécution de ses décisions, non respectées par un responsable du traitement, par une juridiction. Or, si l'article 39 de la loi de 2002 permet au président du tribunal d'arrondissement d'ordonner la cessation d'un traitement de données contraires à la loi, l'article 52 du projet de loi lui permet seulement d'ordonner la suspension provisoire d'un traitement de données contraire au RGPD.

L'article 52 du projet de loi soulève donc toujours des questions quant à l'effectivité et l'utilité de cette action, dans la mesure où une cessation du traitement telle qu'actuellement prévu à l'article 39 paragraphe (1) ne peut pas être ordonnée et que la suspension provisoire du traitement de données, ordonnée par le président du tribunal d'arrondissement, prend fin au plus tard à l'expiration d'un délai de deux ans à partir de la décision initiale de suspension provisoire en vertu du paragraphe (4) de l'article 52.

Cela signifie-t-il qu'un responsable du traitement, ayant violé le RGPD et qui fait l'objet d'une décision de suspension provisoire d'un traitement de données, pourrait recommencer avec le même traitement de données, pourtant illégal, après un délai d'attente de deux ans ?

Ou, l'action étant jugée comme en matière de référé, faut-il comprendre que la CNPD devrait en plus intenter une action judiciaire au fond et dans l'affirmative, devant quel juge ?

L'article 52 mériterait donc d'être précisé eu égard aux questions ci-avant posées.

Il serait également utile de prévoir les modalités sous lesquelles la future CNPD sera autorisée à publier des décisions rendues dans un but dissuasif tel qu'il est déjà prévu en tant que sanction disciplinaire par la loi de 2002 en son article 33 paragraphe 1 (d) qui dispose que la CNPD peut *« ordonner l'insertion intégrale ou par extraits de la décision d'interdiction par la voie des journaux ou de toute autre manière, aux frais de la personne sanctionnée. »* L'article 58 paragraphe 6 du RGPD autorise en effet les États membres à prévoir des pouvoirs additionnels pour son autorité de contrôle.

12. *Autres dispositions*

a) *Disposition modificative*

Une conséquence de l'approche des auteurs du présent projet de loi et de la loi de transposition de la Directive d'avoir opté pour une loi générale et une loi spéciale séparée, est la complexité du changement des références à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel dans toute la législation comportant une telle référence.

Si le présent projet de loi devra toujours être mentionné, la mention de la future loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale, ainsi qu'en matière de sécurité nationale et celle du règlement (UE) 2016/679 doit être appréciée

au cas par cas et la solution retenue ne facilitera pas la lecture de la législation applicable en matière de protection des données personnelles.

b) *Disposition abrogatoire*

Afin d'assurer le respect des dispositions du règlement (UE) 2016/679, une abrogation de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel est inévitable.

Il s'avère qu'un grand nombre de décisions avaient été prises au cours des 15 dernières années sur base de cette loi. Etant donné que le projet de loi ne prévoit rien quant à leur valeur juridique, il y a lieu de présumer que ces actes perdent leur valeur à la date d'abrogation de la loi de 2002, c'est-à-dire à partir du 25 mai 2018.

Dans un souci de sécurité juridique, la CNPD estime nécessaire de prévoir clairement le sort des décisions prises sur base de la loi modifiée du 2 août 2002. Le projet belge prévoit que les autorisations accordées antérieurement gardent leur valeur juridique, sans préjudice des contrôles de la nouvelle autorité.

Pour autant qu'ils ne soient pas contraires aux dispositions de la future loi et du RGPD, la Commission nationale suggère de prévoir p.ex. que les autorisations délivrées sur base des articles 14 et 19 de la loi de 2002 resteraient en vigueur pour une durée de 3 ans, à titre de période transitoire, sans préjudice des pouvoirs de contrôle de la nouvelle CNPD. Pour le surplus, il y a encore lieu de prévoir que les procédures de traitement de demandes d'autorisation en cours introduites avant le 25 mai 2018 sont arrêtées de plein droit.

Pour ce qui est des agréments délivrés aux actuels chargés de la protection des données, sur base de l'article 40 de la loi de 2002, la Commission nationale considère comme nécessaire de prévoir expressément que ces agréments sont abrogés ou annulés à compter de la date d'entrée en vigueur de la loi en projet et au plus tard à partir du 25 mai 2018, pour éviter que des intéressés profitent d'un statut qui n'existera plus.

Conformément aux articles 37 à 39 du RGPD, relatifs au régime du délégué à la protection des données, l'identité du délégué à la protection des données sera dorénavant simplement communiquée à la CNPD, sans obligation de publicité et sans procédure d'agrément ou de certification quelconque. En effet, la loi de 2002 prévoit un régime applicable au chargé de la protection des données qui est purement national, mais qui ne sera plus compatible avec les dispositions du RGPD.

c) *Dispositions transitoires*

L'article 64 prévoit que la durée du mandat des membres du collège nommés avant l'entrée en vigueur du projet de loi sous avis est calculée à partir de la date de nomination de leur mandant en cours lors de l'entrée en vigueur de cette loi. Cette disposition garantit le maintien des droits acquis pour les membres effectifs en fonction à la CNPD actuelle.

Il ne ressort pas explicitement des articles 64 à 67 s'ils s'appliquent aux seuls membres effectifs ou également aux membres suppléants, ce qui ne semble toutefois pas être le cas pour les articles 65 à 67. Pour des raisons de prévisibilité de la loi, il serait prudent de préciser explicitement les catégories de personnes concernées par les articles concernés.

Pour le cas où ces mêmes membres effectifs devraient voir leur mandat renouvelé sous la nouvelle loi, ils risquent de perdre le bénéfice des dispositions des articles 65 et 66 qui pourtant visent à préserver leurs droits acquis. En effet, alors que les articles 64 à 66 visent les membres nommés *« avant l'entrée en vigueur de la présente loi »*, un renouvellement du mandat, c'est-à-dire une nouvelle nomination, pourrait être interprétée comme intervenant sous la nouvelle loi et tombant sous la procédure de l'art 20 de la nouvelle loi.

Afin de renforcer la prévisibilité de la loi pour les intéressés et garantir leurs droits acquis sous la loi actuellement en vigueur, il y a lieu d'ajouter *« nommés pour la première fois avant l'entrée en vigueur de la présente loi »* aux articles 65 et 66. Cet ajout permettrait d'assurer que les membres effectifs actuellement en fonction ne subissent pas une dégradation de leur situation personnelle sans en avoir été informé avant d'accéder à leur fonction sous la loi 2002.

B. Quant à la législation nationale complémentaire

1. *Remarque générale*

La Commission nationale salue l'effort des auteurs de la loi de concilier les intérêts tant des responsables de traitement et sous-traitants que des personnes intéressées dans ce projet de loi élancé, qui dans l'esprit d'harmonisation des législations européennes propagé par le RGPD, limite les dispositions spécifiques nationales à un minium.

2. *Champ d'application des dispositions spécifiques*

Le champ d'application des dispositions spécifiques du Chapitre 2 est défini dans l'article 55 du projet de loi de la manière suivante : *« Les dispositions du présent chapitre s'appliquent aux responsables du traitement et aux sous-traitants établis sur le territoire luxembourgeois »*. Dans le cas où un sous-traitant établi sur le territoire luxembourgeois agit pour le compte et sur instruction d'un responsable du traitement situé en dehors du Luxembourg, il n'est pas clair si ces mesures devront s'appliquer. En effet, l'application de ces mesures aux sous-traitants n'est pas mentionnée dans l'article.

La CNPD estime par ailleurs que dans le cas contraire, un responsable du traitement établi au Luxembourg qui fait appel à un sous-traitant établi hors Luxembourg devra aussi « assurer » que les mesures additionnelles mentionnées à l'article 58 du projet de loi soient appliquées (cf. commentaire ci-dessous).

3. *Traitement à des fins de recherche scientifique ou historique ou à des fins statistiques*

Les articles 57 et 58 du projet de loi limitent les droits des personnes concernées prévus aux articles 15, 16, 18 et 21 du règlement (UE) 2016/679, en conformité avec l'article 89, paragraphe 2, du règlement (UE) 2016/679 moyennant des garanties appropriées. Il y a lieu de constater que les articles 57 et 58 ne couvrent pas les traitements de données à des fins archivistiques dans l'intérêt public tel que le permet pourtant l'article 89 du RGPD. Se pose la question si ces traitements de données ont été exclus intentionnellement par les auteurs du projet de loi ? Le commentaire des articles reste muet sur cette question. La CNPD est donc à se demander si des dérogations ou limitations aux droits des personnes concernées seront, le cas échéant, spécifiquement prévues dans le cadre du projet de loi N° 6913 relatif à l'archivage. Si tel n'était pas le cas, la CNPD donne à considérer que le RGPD s'appliquera aux traitements de données à des fins archivistiques dans l'intérêt public avec toutes les conséquences que cela implique.

La formulation actuelle de l'article 58 stipule que « le responsable d'un traitement » … « doit mettre en oeuvre des mesures appropriées additionnelles ». Or, dans de très nombreux cas, les projets de recherche impliquent un ou plusieurs sous-traitants. La CNPD estime qu'il incombe au responsable du traitement de données de garantir que ces mesures soient mises en place dans les relations contractuelles obligatoires avec le sous-traitant suivant l'article 28 paragraphe (3) du RGPD – ce qui ne signifie pas nécessairement que c'est au responsable de traitement de les mettre en place lui-même. Aussi la CNPD estime que la documentation à laquelle est fait référence au dernier alinéa devra comprendre une analyse au cas par cas pour déterminer quelles mesures s'appliquent au responsable du traitement et quelles mesures s'appliquent au sous-traitant.

4. *Traitement de catégories particulières de données à caractère personnel par les services de la santé*

La section IV comportant un seul article porte le titre *« Traitement de catégories particulières de données à caractère personnel par les services de la santé »*. Comme l'indique le commentaire des articles, l'article 59 est une copie avec quelques ajustements de l'actuel article 7 de la loi modifiée du 2 août 2002.

Si l'article 7 de la loi de 2002 se limitait à réglementer les traitements de données relatives à la santé et à la vie sexuelle par les services de santé, la CNPD s'étonne que l'article 59 du projet de loi couvre dorénavant l'ensemble des catégories particulières de données, données dites « sensibles » visés à l'article 9 paragraphe 1 du RGPD, à savoir :

– les données qui révèle l'origine raciale ou ethnique,

– les opinions politiques,
– les convictions religieuses ou philosophiques,
– l'appartenance syndicale,
– les données biométriques aux fins d'identifier une personne physique de manière unique,
– les données concernant la santé,
– les données concernant la vie sexuelle ou l'orientation sexuelle,
– les données génétiques.

Se pose d'abord la question pourquoi un service de santé – notion qui n'est d'ailleurs pas définie – serait amené à traiter p.ex. des données relatives aux opinions politiques ou à l'appartenance syndicale.

Ensuite, la CNPD s'interroge surtout sur la raison d'être de l'article 59. En effet, si l'article 7 de la loi modifiée du 2 août 2002 doit être lu dans une logique de transposition d'une directive en droit national, en l'occurrence la directive 95/46/CE, il en est autrement s'agissant d'un règlement européen qui s'applique directement dans les Etats membres, sans mesures de transposition. Ainsi, l'article 9 paragraphe 2 lettre h) du RGPD constitue la base juridique (directement applicable en droit national) pour légitimer les traitements de données visés aux paragraphes (1), (3) et (4) dernière phrase de l'article 59 du projet de loi, de sorte que ces dispositions apparaissent superflues et qu'elles peuvent être supprimées du projet de loi.

Pour ce qui est du paragraphe (3) de l'article 59 plus particulièrement, la CNPD se demande en outre pourquoi les entreprises d'assurances, les sociétés gérant les fonds de pension et la Caisse médico-chirurgicale mutualiste (CMCM) y sont énumérées. Ces trois catégories d'organisme peuvent-elles raisonnablement être assimilées à des services de santé ? Enfin, l'on peut aussi se poser la question pourquoi un texte de loi privilégie une société de secours mutuels particulière par rapport à d'autres sociétés de secours mutuels luxembourgeoises. Ces interrogations valent tout aussi bien pour ce qui est de l'actuel article 7 de la loi de 2002.

Le paragraphe (2) de l'article 59 du projet de loi vise les traitements de catégories particulières de données à des fins de recherche. De l'avis de la CNPD ce paragraphe aurait plutôt sa place dans la section III (articles 57 et 58 du projet de loi), alors que celle-ci réglemente plus précisément les traitements de données à des fins de recherches.

Le paragraphe (4) de l'article 59 du projet de loi sous avis est aussi reprise de l'actuel article 7 de la loi de 2002. Cette disposition en projet tout comme l'article 7(4) de la loi de 2002 font référence à un règlement grand-ducal obligatoire qui devrait préciser les modalités et les conditions suivant lesquelles des données « sensibles » peuvent être communiquées à des tiers ou utilisées à des fins de recherche, ce qui correspond en quelque sorte aux *« mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée »* visées à l'article 9 paragraphe 2 lettre j) du RGPD respectivement introduites à l'article 58 du projet de loi. Or, soulignons que jusqu'à ce jour, soit 15 ans après l'entrée en vigueur de la loi modifiée du 2 août 2002, un tel règlement grand-ducal n'a pas été adopté. Un projet de règlement n'a par ailleurs pas été soumis pour avis ensemble avec le projet de loi sous examen. Ceci dit, la CNPD estime que les modalités et les conditions à déterminer par règlement grand-ducal, devraient être précisés dans la loi et non pas dans un règlement grand-ducal, alors que le droit à la protection des données et à la vie privée, s'agissant d'un droit fondamental, est une matière réservée à la loi par la Constitution. A ce titre, il convient de rappeler l'exigence de la Cour constitutionnelle selon laquelle *« dans les matières réservées par la Constitution à la loi, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc. »*[2]

En ce qui concerne la mention de l'utilisation des données « sensibles » à des fins de recherche dans le paragraphe (4) de l'article 59, se pose à nouveau la question de l'agencement et de la cohérence de cette disposition avec celle des articles 57 et 58 du projet de loi.

Enfin, la CNPD regrette et se soucie que le projet de loi ne prévoit pas de règles spécifiques relatives aux traitements des données génétiques. La loi modifiée du 2 août 2002 prévoit actuellement en son article 6 paragraphe (3) un encadrement très strict pour la collecte et l'utilisation des données géné-

2 Arrêt 117 de la Cour constitutionnelle du 20 mars 2015

tiques. La CNPD souligne que ces données sont les plus sensibles qui soient et méritent une protection et encadrement législatif encore plus stricte que les autres données « sensibles ». Tel a aussi été l'avis du législateur en 2002.

L'article 9 paragraphe 4 du RGPD prévoit d'ailleurs expressément que *« Les Etats membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé »*.

En conclusion, la CNPD recommande fortement qu'un encadrement spécifique des données génétiques soit prévu dans la loi, afin de ne pas en abaisser le niveau de protection actuel. Elle suggère par ailleurs de supprimer les paragraphes (1), (3) et (4) dernière phrase de l'article 59 et d'intégrer les dispositions du paragraphe (2) et paragraphe (4) première phrase de l'article 59 dans la section III du projet de loi sous avis.

C. Remarque générale

La Commission nationale regrette que les règlements d'exécution prévues dans le projet de loi n'aient pas été déposées avec loi, voire qu'ils ne lui ont pas été communiqués. Elle n'a par conséquent pas été en mesure de se prononcer à cet égard.

Ainsi décidé à Esch-sur-Alzette en date du 28 décembre 2017.

La Commission nationale pour la protection des données

Tine A. LARSEN	Thierry LALLEMANG	Christophe BUSCHMANN
Présidente	*Membre effectif*	*Membre effectif*

*

AVIS DE L'INSTITUT DES REVISEURS D'ENTREPRISES

(19.10.2017)

Le 12 septembre 2017, le Ministre des Communications et des Médias, Monsieur Xavier Bettel, a déposé à la Chambre des députés le projet de loi 7184 portant création de la Commission nationale pour la protection des données et la mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après le « Projet »).

L'IRE n'entend pas commenter le contexte général et l'opportunité politique du Projet, mais limitera ses propos aux aspects ayant un intérêt particulier pour la profession de réviseur d'entreprises.

Dans ce cadre, l'IRE présente ses observations comme suit :

Généralités

L'IRE souligne qu'un contrôle des comptes annuels, dans la mesure où il est requis par une loi, entre dans le champ d'application de la loi du 23 juillet 2016 relative à la profession de l'audit. En application de la définition présentée à l'article 1 point (6) de cette loi, un tel contrôle est appelé «contrôle légal des comptes ». Tel que mentionné à cette loi, ce contrôle des comptes annuels peut être réalisé que par un « réviseur d'entreprises agréé ».

Il arrive fréquemment que des textes législatifs ou des projets de loi/règlement fassent référence à la profession de réviseur d'entreprises agréé en utilisant, par exemple, des termes comme *« réviseur »*, *« réviseur de comptes »*, *« réviseur agréé »*, *« réviseur externe »*, *« personne agréé à cet effet »*, *« auditeur »*, etc. Il convient donc de corriger la référence au professionnel de l'audit (chapitre XI du Projet) par le terme consacré par la loi du 23 juillet 2016 relative à la profession de l'audit à savoir « réviseur d'entreprises agréé ».

Le présent projet fait référence à la fois aux *« comptes d'exploitation »* ainsi qu'aux *« comptes annuels »*. Toujours au chapitre XI du Projet, il conviendrait d'harmoniser le vocabulaire pour « comptes annuels ».

Il est également à noter que la mission du réviseur d'entreprises agréé n'est pas de certifier exact et complet les comptes annuels mais d'exprimer un opinion sur l'image fidèle de ceux-ci tel que prescrit par les normes internationales d'audit adoptés pour le Luxembourg par la Commission de Surveillance du Secteur Financier chargée de la supervision de la profession de l'audit.

Pour finir, l'IRE remarque que le Projet reste muet sur le référentiel comptable à utiliser pour la tenue de la comptabilité et la préparation des comptes annuels alors que cette précision est apportée dans les lois portant création de plusieurs établissements publics.

Commentaires spécifiques

Article 47

Afin de tenir compte des remarques formulées ci-avant et par analogie à d'autres établissements publics, il est proposé de remplacer le texte de l'article 47 par ce qui suit :

« Art. 47. Les comptes de la CNPD sont tenus selon les règles de la comptabilité commerciale. L'exercice financier coïncide avec l'année civile. Avant le 30 juin de chaque année, le président du collège de la CNPD soumet au collège les comptes annuels comprenant le bilan et le compte de profits et pertes ainsi que l'annexe arrêtés au 31 décembre de l'exercice écoulé, ensemble avec son rapport d'activité et le rapport du réviseur d'entreprises agréé. Le budget annuel de la CNPD est proposé au collège par le président du collège avant le 31 décembre pour l'année qui suit.

Les comptes annuels au 31 décembre de l'exercice écoulé ensemble avec le rapport du réviseur d'entreprises agréé, le rapport d'activité et le budget annuel sont transmis au Gouvernement en conseil qui décide de la décharge à donner à la CNPD. La décision constatant la décharge accordée à la CNPD ainsi que les comptes annuels de la CNPD sont publiés au Journal officiel.

Le Gouvernement en conseil nomme un réviseur d'entreprises agréé sur proposition du collège de la CNPD. Le réviseur d'entreprises agréé a pour mission de vérifier et de certifier les comptes annuels de la CNPD. Le réviseur d'entreprises agréé est nommé pour une période de 3 ans renouvelable. Il peut être chargé par le collège de la CNPD de procéder à des vérifications spécifiques. Sa rémunération est à la charge de la CNPD.

Article 48 paragraphe (2)

L'IRE ne comprend pas pourquoi l'intervention du réviseur d'entreprises agréé est subordonnée à la condition *de ne pas disposer de fonds ne provenant pas de la dotation inscrite au budget de l'Etat.* En application des principes de bonne gouvernance et par analogie à d'autres établissements, il convient de faire contrôler les comptes annuels d'un établissement public et ce sans condition (sauvegarde de l'intérêt public) notamment si l'établissement public est financé partiellement ou totalement par l'Etat. Compte tenu de ce commentaire et de la proposition d'amendement à l'article 47 ci-avant, l'IRE est d'avis que l'article 48 paragraphe (2) devrait être retiré.

Luxembourg, le 19 octobre 2017

Impression: CTIE – Division Imprimés et Fournitures de bureau