Deuxième avis complémentaire de la Commission nationale pour la protection des données relatif aux amendements parlementaires au projet de loi n° 7184 portant organisation de la Commission nationale pour la protection des données et 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), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat

Délibération n° 423/2018 du 8 juin 2018

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 »*.

En date du 28 décembre 2017, la CNPD a adopté un premier avis relatif au projet de loi n° 7184. Un avis complémentaire a été rendu en date du 25 avril 2018.

Suite à une série d'amendements parlementaires, adoptés en date du 14 mai 2018, au projet de loi n° 7184 portant organisation de la Commission nationale pour la protection des données et 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) (ci-après « RGPD »), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat, la CNPD se saisit d'office. Elle entend limiter ses observations dans le présent deuxième avis complémentaire aux amendements n°9, 26, 40 et 41.

Les amendements n° 9 (ancien article 17, nouvel article 14) et n° 26 (ancien article 54)

Le nouvel article 14 prévoit que la CNPD a le « *pouvoir de porter toutes violations des dispositions adoptées en vertu du RGPD* » à la connaissance des autorités judiciaires. La CNPD ne comprend pas le rajout des termes « des dispositions adoptées en vertu du règlement », alors que le paragraphe 5 de l'article 58 du RGPD précise qu'il doit s'agir de « toute violation du présent règlement ». Le nouvel article 14 limite les pouvoirs de la CNPD par rapport au RGPD, sans pour autant préciser quelle juridiction la CNPD est censée saisir.

En l'état, la disposition nationale en question n'a pas de valeur normative, alors qu'elle ne précise pas la procédure judiciaire à suivre par la CNPD pour saisir pro-activement la justice d'une violation du RGPD. Elle avait déjà soulevé cette problématique dans son avis du 28 décembre 2017. Ainsi la CNPD estime que cette question n'est toujours pas suffisamment clarifiée et que la loi en projet n'est pas conforme au RGPD sur ce point.

La Commission nationale regrette par ailleurs que les auteurs des amendements n'ont pas suivi la CNPD dans son avis précité concernant la nécessité de prévoir en droit national une procédure judiciaire telle que l'exige l'arrêt « Schrems » de la CJUE (affaire C-362/14) du 6 octobre 2015. Elle réitère dès lors pour les besoins du présent avissces observations formulées dans son premier avis à ce sujet.

La CNPD regrette aussi que les auteurs des amendements ont supprimé du projet de loi l'ancien article 54. Elle estime qu'en l'absence de ces précisions il y a un risque qu'elle ne pourra pas faire exécuter judiciairement des mesures correctrices adoptés par elle. Ainsi, par exemple, si la CNPD adopterait une mesure correctrice à l'encontre de l'Etat ou d'une commune, elle n'aura pas nécessairement de moyens coercitifs suffisants pour faire respecter sa décision, d'autant plus que le régime des sanctions financières et des astreintes ne s'applique pas à l'Etat ou aux communes.

L'amendement n° 40

L'amendement n° 40 entend remplacer l'article 59 du projet de loi initialement déposé, respectivement l'article 68 du texte coordonné suite aux amendements gouvernementaux du 8 mars 2018. L'amendement propose un nouvel article 63 au Chapitre 3 (du Titre II du projet de loi) intitulé « Traitement de catégories particulières de données à caractère personnel ».

La CNPD voudrait d'emblée relever qu'elle a de sérieux doutes quant à la valeur normative des paragraphes (1), (2) et (3) du nouvel article 63. Malgré les adaptations et modifications textuelles apportées à l'ancien article 68 (article 59 initial), elle ne peut que rappeler et réitérer ses observations formulées dans son premier avis du 28 décembre 2017, à savoir : « *...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.* »

Rappelons que sauf la lettre j) du paragraphe (2), l'article 9 du RGPD ne fait pas partie des « clauses d'ouverture » du Chapitre IX du RGPD (article 85 à 91), c'est-à-dire des « *Dispositions relatives à des situations particulières de traitement* » qui offrent aux Etats membres la possibilité de prévoir et de préciser des règles plus spécifiques dans certaines matières par rapport aux règles générales du RGPD.

Les paragraphes (1), (2) et (3) de l'article 9 du RGPD, applicable en droit luxembourgeois depuis le 25 mai 2018, ne nécessitent donc en principe pas de mesures de transposition telles que celles proposées par les paragraphes (1), (2) et (3) du nouvel article 63 dans le présent projet de loi. Seul le paragraphe (4) de l'article 9 du RGPD permet aux Etats membres de

« *maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé* », auquel la CNPD entend revenir plus loin dans le présent avis.

Ceci dit, la CNPD analysera ci-après les quatre paragraphes du nouvel article 63 du projet de loi.

- Le paragraphe (1) du nouvel article 63 du projet de loi prévoit que le responsable du traitement, lorsqu'il traite des catégories particulières de données pour les finalités prévues à l'article 9 paragraphe 2, lettres b), g) et i) du RGPD, doit mettre en œuvre au moins les cinq mesures de sécurité additionnelles énumérées au points 1° à 5° du paragraphe (1) du nouvel article 63. La CNPD se demande par rapport à quelles autres mesures de sécurité, les mesures de sécurité visées aux point 1° à 5° peuvent être qualifiées d'« *additionnelles* ». Elle suppose qu'il faut comprendre ces mesures de sécurité comme additionnelles par rapport aux mesures de sécurité prévus et requis par les règles du RGPD. Or, les mesures de sécurité proposées dans le texte peuvent tout au plus être considérées comme des mesures standards et ne peuvent manifestement pas être considérées comme additionnelles, alors que l'article 32 du RGPD exige déjà que le responsable du traitement ou le sous-traitant mette en œuvre des mesures de sécurité techniques et organisationnelles appropriées en tenant en compte 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. La CNPD s'étonne dès lors que le texte de loi en projet prévoit un niveau de sécurité qui ne semble pas, dans la grande majorité des cas – sans mesures additionnelles spécifiques - satisfaire le niveau exigé par le RGPD dans le cadre de ces traitements de données hautement sensibles. Elle s'interroge donc sérieusement sur la raison d'être et la valeur normative du paragraphe (1) du nouvel article 63 du projet de loi et estime en tout état de cause que cette disposition est n'est pas conforme au RGPD, de sorte qu'il y a lieu de la supprimer.

- Le paragraphe (2) du nouvel article 63 du projet de loi prévoit que le responsable du traitement, peut communiquer des catégories particulières de données à des tiers pour les finalités prévues à l'article 9 paragraphe 2, lettres b), g), i) et j) du RGPD après avoir mis en œuvre des mesures de sécurité « additionnelles » énumérées au points 1° et 2° du paragraphe (2) du nouvel article 63. Ces mesures de sécurité additionnelles diffèrent de celles du paragraphe (1).

  Tout d'abord, la CNPD s'interroge sur l'utilité de la formulation « *Sous réserve que leur traitement soit en lui-même licite ...* ». Pourquoi faut-il préciser que le traitement initial doit être licite, alors que cela devrait être évident ? Elle se demande, par ailleurs, pourquoi le texte fait référence à la lettre j) du paragraphe 2 de l'article 9 du RGPD (traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques), alors que les traitements de catégories particulière de données dans le cadre de ces finalités sont d'ores et déjà réglés par l'article 62 du projet de loi.

  La CNPD est cependant particulièrement inquiète du contenu et de la portée de la disposition sous revue. Concernant la portée de la disposition :

La disposition semble rendre légitime de facto la communication de catégories particulières de données à caractère personnel à des tiers pour autant que les finalités du traitement par le tiers sont couvertes par l'article 9 paragraphe 2, points b), g), i) et j) du règlement (UE) 2016/679.

En effet, la communication de données sensibles à des tiers constitue une ingérence grave dans la vie privée des personnes concernées. A cet égard, la jurisprudence constante de la CJUE retient que la base légale doit être suffisamment claire et précise et doit offrir une protection contre d'éventuelles atteintes arbitraires, en définissant elle-même la portée de la limitation de l'exercice du droit garanti par la Charte[1]. Pour ce qui est de la notion claire et précise de la base légale, la Cour européenne des droits de l'homme (ci-après « CouEDH ») a énoncé qu'« *on ne peut considérer comme une 'loi' qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé* »[2].

Or, la CNPD est d'avis que la disposition sous avis est très vague et ne respecte pas l'exigence de clarté et de précision de la loi. En effet, le choix des auteurs de l'amendement de l'approche d'ordre fonctionnel au détriment d'une définition d'ordre personnel fait en sorte et comporte le risque que n'importe quel responsable de traitement du secteur public et du secteur privé (administrations, établissements publics, hôpitaux, médecins, laboratoires, asbl du secteur conventionné ,.....) puisse communiquer des données sensibles à n'importe quel tiers, pourvu que la communication des données ait lieu dans le cadre des quatre finalités énumérées, elle-même très générales et vagues et que les mesures de sécurité additionnelles aient été mises en place.

Concernant le contenu de la disposition :

Concernant les soi-disant mesures de sécurité additionnelles, la CNPD tient à constater que la pseudonymisation et le chiffrement des données à caractère personnel font déjà partie des mesures de sécurité explicitement mentionnées dans l'article 32 (1)(a) du RGPD et ne pourront ainsi difficilement être qualifiées de mesures additionnelles en l'occurrence dans le contexte du traitement de catégories particulières de données à caractère personnel. Ceci étant, le point 1° du paragraphe 2 du nouvel article 63 du projet de loi prévoit en premier lieu une anonymisation des données. Or, en réalité et en pratique, dans presque tous les cas l'anonymisation des données est inappropriée, compte tenu de la finalité de la communication des données. Il est en effet difficilement imaginable que le nouveau responsable de traitement puisse effectuer ses traitements sur base de données complètement anonymes. Et si tel était le cas, le RGPD ne s'appliquerait de toute façon pas. Ainsi, le point 1° prévoit en deuxième lieu qu'à défaut d'une anonymisation des données, il y lieu de mettre en place une sécurisation des « *transactions* » telle qu'une pseudonymisation ou un chiffrement des données. La CNPD ne voit pas le lien, ni la logique entre ces deux alternatives, étant donné que la pseudonymisation est une technique de

[1] Cf. l'arrêt du 17 novembre 2015, *WebMindLicenses Kft. c. Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság*, C-419/14, ECLI:EU:C:2015:832, point 81.
[2] Cf. les arrêts de la CouEDH, Sunday Times *c. Royaume-Uni* du 26 avril 1979, série A n° 30, § 61 et CouEDH, *Silver et autres c. Royaume-Uni,* n° 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, série A n° 61, § 86-88.

dépersonnalisation de données utilisée pour que les données ne puissent plus être attribuées à une personne sans avoir recours à des informations supplémentaires et que le chiffrement constitue une pure mesure de sécurité informatique en principe appliquée à des données nominatives.

Ensuite, le point 2° reprend une deuxième fois, qu'à défaut d'une anonymisation des données, il y aurait lieu de prévoir une « *procédure de communication des données assurant la conformité du traitement avec le RGPD* ». La CNPD se demande comment le point 1° s'articule avec le point 2° qui chacun prévoit une alternative en l'absence d'une anonymisation des données. Elle a par ailleurs du mal à saisir ce qu'il faut comprendre par la « procédure de communication » visée au point 2°.

Les mesures ainsi proposées par le texte en projet ne peuvent pas être considérées comme des mesures complémentaires ou additionnelles au régime du RGPD et ne peuvent donc pas en elles seules constituer des garanties appropriées et spécifiques pour la sauvegarde des droits et libertés des personnes concernées au sens du RGPD.

Une « communication de données à des tiers » a bien évidemment aussi lieu lors d'un échange ou partage de données, lors d'une interconnexion de fichiers ou encore lors d'un accès direct à des données d'un fichier. Peu importe donc la terminologie utilisée pour décrire une opération de traitement de données qui comporte toujours une communication de données.

La CNPD tient à rappeler à cet égard 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.* »[3]

Le Conseil d'Etat rappelle lui aussi régulièrement dans ses avis que *« (…) l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.*

La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication (…). »[4]

Sur base de ces considérations, la CNPD estime que la licéité des communications de données sensibles à des tiers devraient se retrouver et être couverte par les différentes lois spéciales réglementant les différents domaines et secteurs visés par les finalités dans le texte sous examen (les lois réglementant la santé publique au sens large, loi sur les établissements hospitaliers, loi réglementant certaines professions de santé, lois réglementant la protection sociale, législation en matière de sécurité sociale, lois réglementant le secteur conventionné, …..), c'est-à-dire que les différentes communications, échanges, partages, interconnexions et accès directs devraient trouver leur légitimité au cas par cas dans ces lois qui devraient préciser les entités ou

[3] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015

[4] Voir par exemple : Conseil d'Etat, Avis n° 6975/5 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.

organismes pouvant communiquer ou se faire communiquer des données et pour quelles finalités précises et spécifiques pour autant que ceci ne ressort pas clairement de leurs missions légales.

La CNPD est d'avis que le paragraphe (2) du nouvel article 63 du projet de loi n'a pas sa place dans un texte de loi général comme celui sous examen, alors qu'il ne répond pas aux exigences de précision et de prévisibilité auxquelles doit répondre un texte légal. Eu égard à l'insécurité juridique importante créée, elle estime nécessaire d'omettre cette disposition.

- Le paragraphe (3) du nouvel article 63 du projet de loi entend légitimer de manière générale des échanges de données dans le cadre de l'accomplissement d'une mission légale ou réglementaire pour une finalité cette-fois ci, à savoir celle indiquée à la lettre h) du paragraphe (2) de l'article 9 du RGPD, « *sous les conditions visées à l'article 9 paragraphe (3) du RGPD* ». La CNPD est à se demander si ce bout de phrase est en l'espèce employé de manière correcte et conforme au RGPD. En effet, à l'endroit de la lettre h) du paragraphe (2) de l'article 9 du RGPD, aux yeux de la CNPD, ce bout de phrase se rapporte uniquement au cas de figure où le « *traitement est nécessaire ..... en vertu d'un contrat conclu avec un professionnel de la santé [et soumis aux conditions et garanties visées au paragraphe 3]* » Le paragraphe (3) de l'article 9 du RGPD n'a dès lors vocation à s'appliquer que dans ce cas de figure particulier. Or, les auteurs de l'amendement entendent généraliser l'application de l'article 9 paragraphe 3 du RGPD à tous les échanges de données visés par la disposition sous examen.

  Pour le surplus la CNPD voudrait se référer et reprendre ici toutes ses observations formulées ci-avant relatives au paragraphe (2) du nouvel article 63 du projet de loi. Ainsi, pour les mêmes raisons, elle estime que le paragraphe (3) du nouvel article 63 du projet de loi devrait être supprimé.

- Le paragraphe (4) du nouvel article 63 du projet de loi a pour objet de limiter le traitement de données génétiques conformément à l'article 9 paragraphe 4 du RGPD qui offre cette possibilité aux Etats membres. Dans son premier avis du 28 décembre 2017, la CNPD s'était souciée que le projet de loi ne contenait pas de dispositions spécifiques relatives aux données génétiques, à l'instar de la loi modifiée du 2 août 2002 sur la protection des données.

  La Commission nationale félicite les auteurs de l'amendement d'avoir intégré les dispositions du paragraphe (4) sous examen pour limiter le traitement de données génétiques et ainsi maintenir le niveau de protection en la matière. Les dispositions s'inspirent largement de l'article 6 paragraphe (3) de la loi modifiée du 2 août 2002 sur la protection des données. La CNPD accueille par ailleurs favorablement l'interdiction du traitement de données génétiques en matière de droit du travail et d'assurance.

- Il est un fait que les compagnies d'assurance doivent pouvoir traiter des données de santé pour certains types de contrats d'assurance. Or, au vu de l'approche fonctionnelle choisi par les auteurs de l'amendement n° 40, les compagnies d'assurance ne se retrouvent plus dans la détermination des responsables de traitement pouvant traiter des données de santé. Il s'avère par ailleurs, qu'aucune des

conditions de légitimité de l'article 9 paragraphe (2) du RGPD n'est susceptible de légitimer le traitement de données de santé par les compagnies d'assurance. La CNPD est d'avis que le consentement explicite prévu à l'article 9 paragraphe (2) lettre a) du RGPD des personnes concernées ne permet pas de légitimer ce traitement de données, alors qu'il pourrait ne pas être considéré comme libre au sens du RGPD pour certains types d'assurance (p.ex. assurance-vie dans le contexte d'un prêt hypothécaire, assurance solde restant dû, ...). De façon générale, un contrat d'assurance étant un contrat d'adhésion, le consentement n'est en règle générale pas considéré comme approprié pour légitimer le traitement de données de santé dans ce contexte. Dans son avis du 30 mars 2018, le Conseil d'Etat a également remarqué à l'endroit de l'article 68 que « *se pose encore la question du consentement des personnes concernées dans le cadre de la conclusion d'un contrat d'adhésion* ». La finalité de la « protection sociale » prévue aux lettres b) et h) du paragraphe (2) de l'article 9 du RGPD n'apparaît pas non plus appropriée pour légitimer le traitement de données de santé par les compagnies d'assurance. En effet, les entreprises d'assurances traitent les données de santé non pas à des fins de santé ou de protection sociale, mais bien à des fins commerciales, comme le précise la Conseil d'Etat dans son avis précité. La protection sociale non autrement définie par le RGPD, n'est pas non plus définie par le droit nationale. Or, la doctrine étrangère analysée par la CNPD constate que les entreprises d'assurance ne font pas partie d'un système de protection sociale nationale lorsque la loi ne le prévoit pas. En effet, les lois françaises et allemandes, par exemple, prévoient expressément que les contrats complémentaires de nature privée d'assurance-maladie sont assimilés à l'assurance-maladie obligatoire et font donc partie du système national de protection sociale. Toujours est-il que les autres types d'assurances indiqués ci-avant ne peuvent pas être considérés comme faisant partie du système de protection sociale. La commission nationale estime donc nécessaire que le projet de loi sous revue prévoit une disposition nationale, conformément à l'article 9 paragraphe (4) du RGPD, pour légitimer le traitement de données de santé en matière d'assurance. Une condition de légitimité appropriée pourrait être celle prévue à l'article 6 paragraphe (1) lettre b) du RGPD. Or, il s'avère que le législateur européen n'a pas prévue cette finalité à l'endroit de l'article 9 du RGPD. La CNPD est d'avis qu'il s'agit là d'un oubli du législateur européen, raison pour laquelle la législation nationale doit remédier à cette carence.

Une telle disposition pourrait voir la teneur suivante : « *Sous réserve des dispositions du règlement (UE) 2016/679, le traitement de données de santé, à l'exception de données génétiques, est licite lorsqu'il est nécessaire à l'exécution d'un contrat d'assurance auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci* ».

L'amendement n° 41 (nouvel article 63 bis)

L'amendement n° 41 introduit par l'article 63bis une nouvelle disposition pour limiter les pouvoirs d'accès de la CNPD lui conférés par le RGPD par les lettres e) et f) du paragraphe (1) de l'article 58.

La CNPD estime que la disposition en question ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal, alors que le texte ne précise pas exactement quels lois ou règlements régissant les professions soumises au secret professionnel doivent être respectés. Par ailleurs, pas toutes les lois qui soumettent une

profession au secret ne prévoient une procédure spécifique dans le cadre d'enquêtes administratives ou judiciaires. En tout état de cause, la CNPD comprend que dans les cas où la législation ne prévoit pas de règles de procédures spécifiques d'accès aux locaux et aux données, le pouvoir d'enquête de la CNPD ne peut pas être limité, c'est-à-dire que le secret professionnel ne peut lui être opposé. Elle estime qu'en l'état, la disposition nationale en projet ne concilie pas le droit à la protection des données et l'obligation de secret qui s'impose à certaines professions.

Ainsi décidé à Esch-sur-Alzette en date du 8 juin 2018.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	Christophe Buschmann Membre effectif