N° 8331[3]

CHAMBRE DES DEPUTES

PROJET DE LOI

portant modification de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique

* * *

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(23.2.2024)

1. Conformément à l'article 57.1.c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après le « RGPD »), auquel se réfère l'article 7 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la Commission nationale pour la protection des données (ci-après la « Commission nationale » ou la « CNPD ») « *conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ».

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

Le Comité européen de la protection des données (ci-après le « CEPD ») précise par ailleurs que pour toute limitation aux droits des personnes concernées adoptée au niveau des États membres, l'autorité de contrôle en matière de protection des données doit être consultée avant l'adoption d'une telle mesure par le parlement national[1].

2. Par courrier en date du 20 octobre 2023, le Ministère de la Santé a invité la Commission nationale à se prononcer sur le projet de loi n°8331 portant modification de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique (ci-après le « projet de loi »). Par ailleurs, ledit Ministère a saisi la CNPD par courrier du 25 octobre 2023 afin d'aviser le projet de règlement grand-ducal précisant les modalités et conditions de mise en place du carnet de vaccination électronique (ci-après le « projet de règlement grand-ducal »). Le projet de règlement grand-ducal est pris en exécution du futur article 4*bis* de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique et la mise en œuvre d'un carnet de vaccination électronique[2] (ci-après le « futur article 4*bis* de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies »), tel qu'inséré après l'article 4 de ladite loi par l'article 2 du projet de loi susmentionné.

---

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

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

3. Bien que la Commission nationale ne souhaite nullement remettre en cause l'utilité de la mise en place d'un carnet de vaccination sous forme électronique (ci-après le « carnet digital ») visant à remplacer le carnet physique, dit « carte jaune », et ceci « *tant pour le bénéfice du patient que pour l'amélioration de l'efficacité et de la transparence des campagnes nationales de vaccination* »[3], elle souligne cependant que des garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données à caractère personnel doivent être mises en œuvre.

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

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

5. Par ailleurs, dans la mesure où une partie des données traitées à travers le carnet digital sont relatives à la santé des patients en cause, celles-ci sont à qualifier de catégories particulières de données, dites « données sensibles », au sens de l'article 9 du RGPD. De tels traitements requièrent une protection spécifique et sont soumis à des exigences plus strictes. Le traitement de données sensibles est, en effet, interdit sauf si l'une des conditions visées au paragraphe 2 de l'article 9 du RGPD est remplie.

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

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

I. Quant au responsable du traitement

7. La CNPD tient à rappeler que conformément à l'article 4.7) du RGPD, le responsable du traitement est « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre*. »

8. En ce qui concerne plus précisément les notions de responsable du traitement et de sous-traitant, il ressort des lignes directrices du CEPD sur ce sujet que « *[l]orsque le responsable du traitement est spécifiquement identifié par la loi, cette désignation est déterminante pour définir qui agit en tant que*

---

3 Voir exposé des motifs du projet de loi.

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

responsable du traitement. Cela présuppose que le législateur a désigné comme responsable du traitement l'entité qui est véritablement en mesure d'exercer le contrôle. »[5]

9. Il est encore à noter que la notion de responsable du traitement, voire de responsabilité conjointe, sont des notions fonctionnelles en ce qu'elles visent à répartir les responsabilités en fonction des rôles réels joués par les parties. Ainsi, elles reposent sur une analyse factuelle plutôt que formelle.[6]

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

11. Le texte du projet de loi engendre dès lors l'impression que l'Agence eSanté, créée sur base de l'article 60*ter* du Code de la sécurité sociale et soumise à l'autorité conjointe des ministres ayant dans leurs attributions la Santé et la Sécurité sociale, agirait seule en tant que responsable du traitement des données à caractère personnel opéré dans le cadre de la mise en œuvre du carnet digital. Néanmoins, la CNPD constate que des précisions se trouvent à cet égard dans le projet de règlement grand-ducal, ainsi que dans son commentaire des articles[7]. D'après sa lecture, il en ressort la configuration suivante :

– L'Agence eSanté sera responsable des traitements des données opérés par la création même du carnet digital pour chaque personne physique disposant d'un numéro d'identification national[8] et ceci à partir du premier encodage par le prestataire de soins. Par ailleurs, en vertu de l'article 1er (4) du projet de règlement grand-ducal, l'Agence eSanté doit procéder, dès réception d'un certificat de décès ou de la date de décès par le Centre des technologies de l'information de l'Etat, à l'archivage des données du carnet digital pendant la durée légale de conservation.
– Pour le traitement des données enregistrées par les prestataires de soins dans le carnet digital,[9] l'article 2 (1) du projet de règlement grand-ducal prévoit que lesdits prestataires agissent comme responsables conjoints avec l'Agence eSanté au sens de l'article 26 du RGPD.
– Finalement, pour le traitement des données enregistrées par l'autorité sanitaire[10] sur la gestion des stocks de vaccins et qui peuvent inclure des données à caractère personnel des prestataires de soins,[11] l'article 2 (2) du projet de règlement grand-ducal prévoit que l'autorité sanitaire agit avec l'Agence eSanté comme responsables conjoints au sens de l'article 26 précité du RGPD.

---

5 CEPD, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.0, adoptées le 7 juillet 2021, point 23.

6 Page 3 et points 21 et 52 desdites lignes directrices.

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

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

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

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

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

12. La CNPD a néanmoins des difficultés à relier les traitements précités opérés par les différents acteurs aux finalités mentionnées au futur article 4*bis* (2) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies. En d'autres termes, elle est d'avis qu'il ne ressort pas clairement des textes sous avis pour quelles des différentes finalités poursuivies l'Agence eSanté, l'autorité sanitaire, ainsi que les prestataires de soins de santé sont à considérer comme responsable, voire comme responsables conjoints des traitements mis en œuvre à travers le carnet digital.

13. Dès lors, en prenant en compte que la protection des données à caractère personnel est une matière réservée à la loi par la Constitution, d'une part, et que dans de telles matières l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc,[12] la Commission nationale recommande aux auteurs du projet de loi de préciser dans le corps du texte qui est à qualifier de responsable, voire de responsable(s) conjoint(s) des traitements en distinguant entre les différentes finalités à atteindre.

14. Finalement, il convient de mentionner que l'article 26.1 du RGPD dispose que les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du RGPD, notamment en ce qui concerne l'exercice des droits de la personne concernée. Les lignes directrices du CEPD à ce sujet prévoient qu'il « *convient de répartir les responsabilités en matière de conformité, ainsi qu'il résulte de l'utilisation du terme « respectives » à l'article 26, paragraphe 1. Cela n'exclut pas que le droit de l'Union ou le droit d'un État membre puisse déjà établir certaines responsabilités de chaque responsable conjoint du traitement. Si tel est le cas, l'accord entre les responsables conjoints du traitement devrait également couvrir toute responsabilité supplémentaire nécessaire aux fins d'assurer le respect des exigences du RGPD qui ne sont pas couvertes par les dispositions légales*. »[13]

15. Les paragraphes (3) et (4) de l'article 2 du projet de règlement grand-ducal précisent dans ce contexte les modalités d'exercice des droits des personnes concernées. La CNPD tient dès lors à rendre attentifs les auteurs du projet de règlement grand-ducal qu' « *[i]l ne s'agit que de définir, dans leurs relations internes, quelle partie est tenue de répondre aux demandes des personnes concernées*. »[14] En effet, indépendamment des termes de l'accord entre responsables conjoints, la personne concernée peut contacter chacun des responsables conjoints du traitement conformément à l'article 26.3 du RGPD.

II. Quant aux données à caractère personnel collectées

16. Au titre du respect des principes relatifs au traitement des données à caractère personnel tels qu'ils sont prévus par le RGPD, la CNPD rappelle que les données à caractère personnel doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités […] (limitation des finalités)* » et qu'elles doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)*. »[15]

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

---

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

13 Point 162 desdites lignes directrices.

14 Point 165 desdites lignes directrices,

15 Voir article 5.1.b) et e) du RGPD.

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

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

19. Par ailleurs, la CNPD note que le futur article 4*bis* (5) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies prévoit que les données des personnes vaccinées contre la COVID-19[16] sont transférées au carnet digital. Elle comprend que ce transfert se justifie, notamment afin que les personnes continuent à bénéficier d'une preuve de vaccination en cas de dommages ou de demandes de suivi d'effets indésirables et leur permet de garder trace de leur vaccination contre la COVID-19.[17]

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

20. Finalement, comme le futur article 4*bis* (4) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies prévoit que le patient doit consentir à l'enregistrement des données relatives aux futures vaccinations autres que celles recommandées par l'Etat, la CNPD tient à insister que toutes les conditions d'un consentement valide au sens du RGPD sont à respecter, notamment que le consentement doit être libre, spécifique, éclairé et univoque.[18]

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

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

---

16 Traitées sur base de l'article 10 (2), point 3°, point b) de la loi modifiée du 17 juillet 2020 portant introduction d'une série de mesures de lutte contre la pandémie Covid-19.

17 Voir commentaire des articles du projet de loi, ad article 2.

18 Voir définition du consentement à l'article 4 point 11 du RGPD, ainsi que les conditions applicables au consentement prévues à l'article 7 du RGPD.

grand-ducal du 6 décembre 2019 précisant les modalités et conditions de mise en place du dossier de soins partagé est à appliquer.

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

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

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

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

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

25. La CNPD constate avec satisfaction que l'article 4.1 du projet de règlement grand-ducal prévoit un système de journalisation des accès, c'est-à-dire un enregistrement des données d'identification de la personne qui a consulté ou enregistré une ou plusieurs données au carnet digital, ainsi que le contexte de son intervention. Selon ledit article, les « *données de journalisation suivent le même cycle de vie que les données auxquelles elles se rapportent* », c'est-à-dire que la durée de conservation des logs est la même que celle des données du carnet digital.[19] Comme le futur article 4*bis* (8) de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies prévoit que les données contenues dans le carnet digital sont sauvegardées pendant trente ans suite à leur encodage par le prestataire de soins, il en ressort que les données de journalisation seraient conservées aussi pendant trente ans.

26. Néanmoins, alors que les fichiers de journalisation peuvent être considérés comme un élément servant à remplir l'obligation de sécurité découlant de l'article 32 du RGPD en évitant des accès

19 Voir commentaire des articles du projet de règlement grand-ducal, ad article 4.

non-autorisés aux données à caractère personnel, les données de ces fichiers permettant d'identifier des personnes ne doivent, comme toutes les données à caractère personnel, pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées conformément à l'article 5.1.e) du RGPD.

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

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

Or, la Cour de justice de l'Union européenne a estimé que « *la durée de conservation des données de base peut constituer un paramètre utile sans toutefois être déterminant* ». Par ailleurs, elle a décidé qu' « *une réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêts et obligations en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement* ».[20]

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

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

IV. Quant au droit d'opposition

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

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

---

20 CJUE, arrêt du 7 mai 2009, C-553/07, EU:C:2009:293, points 58 et 66.

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

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

Par ailleurs, il y a lieu de soulever que lorsqu'une telle restriction aux droits des personnes est prévue par une mesure législative, elle doit contenir des dispositions spécifiques relatives aux informations énumérées au paragraphe 2 de l'article 23 du RGPD.[22]

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

34. Le CEPD a clarifié que la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme exigent que « *les mesures législatives qui visent à limiter l'étendue des droits des personnes concernées ou des obligations du responsable du traitement soient prévisibles pour les personnes concernées.* »[23] De même, l'analyse et le constat de nécessité et de proportionnalité d'une limitation sur base d'une mesure législative devraient être effectués par le législateur avant qu'il décide de prévoir une restriction.[24]

Par ailleurs, « *[l]e lien entre les limitations prévues et l'objectif poursuivi devrait être clairement indiqué dans la mesure législative*. »[25].Ce lien doit donc y être expressément précisé.

35. La CNPD note que d'après les auteurs du projet de loi et leur commentaire des articles, la mesure de limitation du droit d'opposition des personnes concernées constitue une mesure nécessaire et proportionnée afin de garantir la réalisation des finalités de santé publique pour lesquelles le carnet digital est mis en place, en particulier la détermination du taux de couverture vaccinale, ainsi que la traçabilité et la gestion des stocks de vaccins distribués par l'Etat. Elle comprend dès lors que ladite limitation pourrait viser à garantir un objectif important d'intérêt public dans le domaine de la santé publique conformément à l'article 23.1.e) du RGPD.

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

---

21 Voir article 21.1, deuxième phrase du RGPD.

22 Il s'agit des finalités du traitement ; des catégories de données à caractère personnel; de l'étendue des limitations introduites ; des garanties destinées à prévenir les abus ou l'accès ou le transfert illicites; la détermination du responsable du traitement; les durées de conservation et les garanties applicables ; les risques pour les droits et libertés des personnes concernées et le droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation.

23 Lignes directrices du CEPD concernant les limitations au titre de l'article 23 du RGPD, point 17.

24 Lignes directrices du CEPD concernant les limitations au titre de l'article 23 du RGPD, point 40.

25 Lignes directrices du CEPD concernant les limitations au titre de l'article 23 du RGPD, point 21.

36. En ce qui concerne les finalités du traitement[26], il s'agit de préciser pourquoi le droit d'opposition de la personne concernée est limité (et pas les finalités du traitement opéré en général). La disposition sous revue doit être compréhensible pour les personnes auxquelles elle s'applique, ce qui implique une compréhension claire de comment et quand la limitation s'applique.

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

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

37. Finalement, le CEPD est d'avis qu'« *une exclusion générale des droits des personnes concernées à l'égard de l'ensemble ou de certaines opérations de traitement de données ou à l'égard de certains responsables du traitement ne respecterait pas l'essence du droit fondamental à la protection des données à caractère personnel tel qu'il est consacré par la Charte* ».[27]

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

– *l'exclusion, pour un même traitement, de l'ensemble des droits prévus par le RGPD*
– *tout comme l'exclusion générale du droit d'opposition pour tous les traitements mis en œuvre par une collectivité publique.* »[28]

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

Ainsi adopté à Belvaux en date du 23 février 2024.

La Commission nationale pour la protection des données

Tine A. LARSEN *Présidente*	Thierry LALLEMANG *Commissaire*
Marc LEMMER *Commissaire*	Alain HERRMANN *Commissaire*

26 Prévu par l'article 23.2. point a) du RGPD.

27 Lignes directrices du CEPD concernant les limitations au titre de l'article 23 du RGPD, point 14.

28 Article de la CNIL « *Droit d'opposition : les conditions de dérogation en vertu de l'article 23 du RGPD* » du 1er juin 2023, disponible sous : « https://www.cnil.fr/fr/droit-dopposition-les-conditions-de-derogation-en-vertu-de-larticle-23-du-rgpd.

Impression: CTIE – Division Imprimés et Fournitures de bureau