Avis n°106/2018 du 17 octobre 2018

Objet : Avis d'initiative - Audition de l'Autorité de protection des données sur le projet de la loi portant des dispositions diverses concernant le Registre national et les registres de population – DOC 54 3256 - Suivi de l'avis 19/2018 de la CPVP (CO-A-2018-132)

L'Autorité de protection des données (ci-après l'Autorité);

Vu la loi du 3 décembre 2017 *relative à la loi portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26;

Vu le rapport de Monsieur Willem Debeuckelaere;

Émet, le 17 octobre 2018, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. La Commission des Affaires Intérieures du Parlement a invité l'Autorité de protection des données pour une audition en date du 16 octobre 2018 sur le projet de la loi portant des dispositions diverses concernant le Registre national et les registres de population – DOS 54 3256.

2. L'autorité de protection des données s'est prononcée sur l'avant-projet de loi portant des dispositions diverses « Intérieures » aux termes de son avis 19/2018 du 28 février dernier.

3. Dans la mesure où ce projet de loi comporte des mesures présentant un impact important sur les droits et libertés des personnes concernées, l'Autorité émet d'initiative le présent avis afin d'analyser le suivi qui a été fait de son avis précité 19/2018. Sur de nombreux points, le projet de loi portant des dispositions diverses concernant le Registre national et les registres de population (ci-après « le projet de loi ») suit l'avis 18/2018 de la Commission de protection de la vie privée (CPVP). Au vu du temps limité dont dispose l'Autorité de protection des données (APD), le présent avis se limite à aborder les points non suivis de l'avis 18/2018 de la CPVP ainsi que, sans nécessairement tendre à l'exhaustivité, des remarques sur des nouvelles dispositions présentant un impact négatif en terme de garanties pour les personnes concernées quant à leur niveau de protection de leur droit fondamental à la protection des données à caractère personnel.

4. L'attention des parlementaires est particulièrement attirée sur l'article 27 du projet de loi qui prévoit l'insertion des empreintes digitales dans la puce électronique de la carte d'identité. Vu l'impact de cette mesure au regard du droit fondamental à la protection des données à caractère personnel, une chapitre spécifique a été rédigé sur le sujet. Il figure à la fin du présent avis.

II. EXAMEN QUANT AU FOND

5. Il ressort de l'art. 2, §2 du projet de loi que de nouveaux sous-registres peuvent être créés par le Registre national (ci-après « RN »). La rédaction de cette disposition ne répond pas aux critères de prévisibilité et de qualité des lois encadrant des traitements de données à caractère personnel énoncés par la Cour européenne des droits de l'Homme. **L'article 2,§ 2 doit préciser explicitement quels sont ces sous-registres** autres que ceux déjà visés à l'article 2 §1 en projet de la LRN (Registres de population, registres des étrangers, registre d'attente et registres consulaires) et à l'article 6bis de la loi de 1991 sur les Registres de population (Registre des cartes d'identité et Registre des cartes d'étranger)**. Selon les explications reprises à l'exposé des**

motifs, il semble s'agir du Registre de Protocole et du nouveau sous-registre créé par le présent projet de loi, le **Registre des personnes figurant sur un acte de l'état civil belge**.

6. Concernant la création de ce nouveau **Registre des personnes figurant sur un acte de l'état civil belge, le flou entoure sa création sur plusieurs aspects ; ce qui doit être corrigé pour répondre aux critères de qualité requis** :
    a. Il convient de **préciser limitativement les actes d'état civil concernés.**

    b. En outre, la **justification de la création de ce dernier Registre doit apparaitre clairement dans l'exposé des motifs sans quoi il ne peut faire l'objet d'une analyse de légitimité et de proportionnalité**.
        i. **En quoi le fait de figurer dans un acte de l'état civil justifie la mention de la personne dans le RN au regard des finalités du Registre national ?**
        ii. **A priori, la raison d'être de l'inscription d'une personne dans le Registre national est liée aux contacts répétés que cette personne va avoir avec les administrations belges. Est-ce que ce critère est rempli pour toute personne figurant dans un acte de l'état civil ?**

    c. Outre la problématique de l'absence de justification concrète de la création de ce nouveau registre, **l'article 2, § 4, 3° en projet de la LRN décrit les nouvelles catégories de personnes à inscrire dans ce registre de façon floue et difficilement praticable** (*« les personnes qui sont mariées* ***ou qui envisagent de contracter mariage*** **(Critère trop flou et non vérifiable)** *avec une personne inscrite au RN, qui cohabitent* **(de fait ou légale ?)** *ou* ***qui envisagent de faire*** **(*Critère trop flou et non vérifiable)*** *une déclaration de cohabitation légale avec une personne inscrite au RN, ou* ***qui sont concernées par une reconnaissance*** **(De quels types de reconnaissance parle-t-on?)***, mais qui ne disposent pas d'un numéro de RN* ») Au de l'article 22 de la Constitution, ce n'est pas au Roi mais au législateur de déterminer de manière exhaustive et déterminée les personnes concernées par une inscription dans ce registre centralisé.

    d. Les mêmes remarques peuvent également être faites à propos l'article 5 du projet de loi qui insère un nouvel article 2ter dans la LRN « Sont mentionnées au Registre national, à partir d'une date déterminée par le ministre de l'Intérieur, les personnes physiques mentionnées sur un acte d'état civil belge établi par un officier de l'état civil mais qui ne font pas l'objet d'une inscription ou d'une mention dans le

Registre national des personnes physiques à un autre titre » **Quels sont les actes d'état civil concernés et quelle est la justification ?**

e. Selon l'article 9 du projet de loi, les données de ce registre (« Etat civil ») seront uniquement conservées à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques d'intérêt général. Il y a là une **contradiction avec l'article 2 de la LRN** qui décrit d'autres finalités pour lesquelles les données du RN peuvent être utilisées. Ce point doit être éclairci (en plus des justifications nécessaires visées ci-dessus).

f. **Ce même article précise les données relatives à ces personnes qui seront reprises dans le Registre national mais de façon partiellement variable,** à savoir les données visées à l'article 3, al. 1er 1° à 3° de la LRN et les autres données visées à l'article 3 de la LRN pour autant qu'elles soient disponibles dans l'acte d'état civil concerné. Cela n'est **pas compatible avec les critères de qualité et de prévisibilité de la CEDH** et risque d'être jugé contraire à l'article 10 de la Constitution. Les données à caractère personnel qui seront centralisées dans ce registre doivent être déterminées par la loi de manière limitative.

7. L'article 10 du projet de loi modifie l'article 5 de la LRN pour l'adapter suite à la suppression du Comité sectoriel intégré au sein de la Commission de protection de la vie privée. C'est dorénavant le Ministre de l'intérieur qui procédera aux **autorisations d'accès au Registre national et d'utilisation du numéro d'identification du numéro de RN** ; ce qui cadre avec son rôle de responsable de traitement de ce Registre.

a. **Le projet de loi fait, dans plusieurs de ses articles** (cf. notamment art. 10 et 11)**, référence aux conditions et modalités de l'autorisation d'accès au RN** ***« prévues au § 1er de l'article 5 § 1 en projet »***. **Or, ces conditions figurent à l'article 15 de la LRN en projet et sont réduites par rapport aux conditions qui sont actuellement prévues dans la LRN aux alinéas 2 et 3 de l'article 5 de la LRN. Il convient d'une part, de corriger la référence faite** (en visant également l'article 15 futur de la LRN) **et d'autre part, de compléter les conditions** et modalités de l'autorisation visées à l'article 15 en projet de la LRN **par ces termes « la vérification si l'accès aux données demandées et l'utilisation du numéro de RN demandé sont conformes au RGPD ».** Il s'agit d'une prérogative du Ministre de l'Intérieur en tant que responsable de traitement du Registre national.

b. **Quant à la vérification des mesures de sécurité adoptées par les utilisateurs du Registre national, l'exposé des motifs précise que le Ministre ne procédera à aucune vérification préalable en la matière et qu'il s'agit de la mission de l'Autorité de protection des données.** Que ce soit pour l'Autorité de protection des données dans l'exercice de ses compétences de contrôle ou pour le Ministre de l'Intérieur dans l'exercice de sa compétence de vérification des conditions pour pouvoir être autorisé à accéder aux données du Registre national, il est vrai que les **moyens à mettre à leur disposition pour être mesure d'auditer sur place les mesures de sécurité** adoptées par **tous les utilisateurs du Registre national** devraient être **très élevés et couteux**.

Il convient donc que le législateur précise explicitement les exigences de sécurité minimales requises des utilisateurs du Registre national. Cela donnera une ligne de conduite claire en la matière à leur attention et les responsabilisera quant aux mesures à prendre. Pour ce faire, le législateur pourrait par exemple s'inspirer des formulaires qui étaient utilisés par le Comité sectoriel du Registre national **en exigeant des demandeurs d'autorisation une déclaration sur l'honneur selon laquelle ils remplissent les conditions minimales suivantes à reprendre dans la LRN:** (1) La réalisation d'une évaluation des risques encourus par les données à caractère personnel traitées et la définition des besoins de sécurité en conséquence, (2) la tenue d'une version écrite de la politique de sécurité de l'information précisant les stratégies et mesures retenues pour sécuriser les données à caractère personnel traitées, (3) l'identification de tous les supports impliquant des données à caractère personnel traitées, (4) l'information du personnel interne et externe impliqué dans le traitement des données quant à ses devoirs de confidentialité et de sécurité vis-à-vis des données traitées découlant tant des dispositions légales que de la politique de sécurité, (5) l'adoption de mesures de sécurisation physique des données pour prévenir les accès physiques inutiles ou non autorisés aux supports contenant les données à caractère personnel traitées, (6) l'adoption de mesures de sécurité physique et environnementale pour prévenir les dommages physiques pouvant compromettre les données à caractère personnel traitées, (7) l'adoption de mesures de protection des réseaux auxquels sont reliés les équipements traitant les données à caractère personnel, (8) la tenue d'une liste actualisée des différentes personnes habilitées à accéder aux données à caractère personnel dans le cadre du traitement précisant et justifiant leur niveau d'accès respectif au regard de leur fonction exercée (création, consultation, modification, destruction), (9) la mise en place d'une sécurisation logique des accès aux données via un mécanisme d'autorisation d'accès conçu de façon à ce que les données à caractère personnel traitées et les traitements les concernant ne soient accessibles

qu'aux personnes et applications explicitement autorisées, (10) la mise en place d'une journalisation des accès tel que soient réalisés un traçage et une analyse permanente des accès des personnes et entités logiques aux données à caractère personnel, (11) la mise en place d'un contrôle de la validité et de l'efficacité dans le temps des mesures techniques ou organisationnelles implémentées, (12) la mise en place de procédures de gestion d'urgence des incidents de sécurité impliquant les données à caractère personnel traitées, (13) la constitution et tenue à jour d'une documentation suffisante concernant l'organisation de la sécurité de l'information dans le cadre du traitement en question.

c. **Enfin, il convient de coordonner l'exigence d'autorisation préalable par Arrêté ministériel avec l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel** qui prévoit que « sauf autre disposition dans les lois particulières, en exécution de l'article 6.2 du RGPD, l'autorité publique fédérale qui transfère des données à caractère personnel sur base de l'article 6.1.c ou 6.1.e du RGPD, formalise cette transmission par chaque type de traitement par un **protocole** entre le responsable de traitement initial et le responsable de traitement destinataire des données ».

8. L'article 5, §2 en projet de la LRN confère au Ministre le pouvoir d'autoriser les **accès aux données des Registres de population, via les services du RN**. Il est précisé, comme c'est déjà le cas actuellement dans la LRN, que ces données ne sont pas conservées au Registre national.

   Il convient de **corriger cette fiction** dans la mesure où il est impossible de servir d'intermédiaire dans un flux de données sans conserver un minimum de temps les données concernées. Selon l'exposé des motifs, il est précisé qu'il faut comprendre cette formulation de façon telle qu'il ne faut pas considérer les données des Registres de population accédées via les services du Registre national comme *des données « légales » au sens de la LRN.* **Qu'est-ce que cela signifie concrètement et quelles en sont les conséquences concrètes en terme de traitement de ces données et d'accessibilité ?**

9. **L'article 5ter de la LRN en projet prévoit l'ouverture du Registre national au secteur privé pour la mise à jour de leurs fichiers ou banques de données signalétiques de clientèle moyennant rémunération des services du Registre national**.

   a. La plupart des remarques faites à ce sujet par la CPVP ont été suivies à l'exception de celles concernant la nécessité d'imposer l'adoption de mesures de sécurité minimale aux organismes privés et publics qui seront concernés par la réception des mutations

du Registre national sur cette base. L'article 5ter, §2, 6° en projet prévoit uniquement l'obligation de désigner un délégué à la protection des données ainsi que la tenue à la disposition de l'autorité de protection des données d'un « plan de sécurité des données » sans autre précision. **Au vu du caractère totalement insuffisant de cette dernière mesure, il convient en lieu et place que le législateur précise les conditions minimales de sécurité auxquelles ces organismes devront satisfaire pour recevoir les actualisations de données. Il est à ce sujet renvoyé au point 7.b ci-dessus**. Un engagement sur l'honneur de l'adoption de ces mesures pourrait être prévu par le législateur.

b. **L'article 5ter, §2, 3° en projet devrait être corrigé car exiger la suppression des données d'identification de base de la personne concernée dès la fin du contrat n'est potentiellement pas conforme au RGPD.** A titre d'exemple, e**n** cas de gestion de contentieux relatif à ce contrat, une conservation plus longue peut être justifiable et conforme au RGPD. Les termes « en tout état de cause, les données doivent immédiatement être détruites dès la fin du contrat » devraient être supprimés.

c. **Pour assurer le caractère effectif de l'obligation pour les organismes concernés de signaler aux services du RN la cessation de la relation contractuelle pour laquelle les mutations des données du RN leur seront communiquées, prévue à l'article 5ter, §3, il convient de prévoir une sanction pénale spécifique de son non-respect.** Cette obligation est importante au regard du droit à la protection des données à caractère personnel car elle assure le caractère légitime du flux de données visé dans le temps. Sans cette sanction pénale spécifique, il y a un risque certain que cette obligation reste lettre morte et que les services du Registre national continueront à communiquer à ces organismes des données non pertinentes et sans base de légitimité.

La même remarque vaut pour l'article 5ter, §5 de la LRN en projet qui interdit la vente, la communication aux tiers et l'utilisation à des fins publicitaires des données qui seront mises à disposition des organismes sur base de cet article 5ter en projet.

d. **L'article 5ter § 4 de la LRN en projet prévoit que la «** *liste de l'ensemble des organismes autorisés par les personnes physiques à recevoir automatiquement du RN les modifications intervenues sur leurs données ainsi que les finalités pour lesquelles lesdites modifications sont communiquées est établie, tenue à jour et disponible sur*

le site internet du Registre national » **.** Dans la mesure où la détermination de ces organismes et lesdites finalités de communication de données sont liées au consentement de chaque personne concernée, cette liste peut uniquement être accessible pour chaque personne physique et non publiquement sur internet. Si l'intention du législateur est de communiquer les noms des organismes qui souhaitent bénéficier potentiellement de ce système, il convient de reformuler en ce sens cette disposition pour qu'elle reflète correctement l'intention du législateur. **Dans sa formulation actuelle, la publication envisagée par l'article 5ter §4 de la LRN en projet consistera en un traitement de données à caractère personnel contraire au RGDP**.

10. Afin d'assurer un niveau de sécurité minimal correct des utilisateurs du Registre national, **l'article 10 de la LRN en projet doit préciser quelles sont les mesures de sécurité minimales requises**. Il est renvoyé au point 7.b. du présent avis.

11. Le projet de loi supprime l'article 12 § 2 actuel de la LRN qui impose à tout bénéficiaire d'une autorisation d'un accès au RN de désigner nominativement leurs organes ou préposés qui en raison de leurs attributions disposent d'un accès au RN et de tenir à jour la liste actualisée de ces personnes. **Aucune justification n'est reprise dans l'exposé des motifs quant à cette suppression alors que cette obligation oblige les utilisateurs du Registre national à limiter les membres de leur personnel habilités à consulter le Registre national au strict nécessaire.**

12. L'autorité constate avec satisfaction l'instauration de l'obligation légale de tenue de fichiers de journalisation correcte des accès au Registre national (loggings) par les utilisateurs du Registre national ainsi que la pénalisation du non-respect de cette obligation. Cela va améliorer grandement la situation à laquelle la CPVP a souvent été confrontée lors de ses contrôles sur des soupçons d'utilisation illégale des données du Registre national ; les responsables de traitement avançant souvent l'impossibilité de vérifier qui a utilisé les données vu l'absence de logging.

    En plus de prévoir cette obligation de journalisation, **l'article 17 alinéa 5 en projet de la LRN** prévoit la tenue par les services du RN d'un registre des consultations des utilisateurs et communications effectuées avec indication de l'identification de l'utilisateur qui a accédé aux données, des données consultées et de la date et heure de consultation. Comme pour tout traitement de données à caractère personnel spécifiquement encadré par la loi, il convient de **préciser la finalité concrète pour laquelle ce registre interne est créé**.

13. Sur l'article 27 du projet de loi qui modifie l'article 6 de la loi de 1991 sur les Registres de population (loi de 1991) en prévoyant notamment l'insertion des empreintes digitales, il est renvoyé au chapitre du présent avis consacré spécifiquement à ce sujet (points 19 et suivants).

14. L'article **6 § 4 en projet** de la loi de 1991 **règlemente la lecture et l'enregistrement des données figurant sur la carte d'identité** en prévoyant que toutes les données y figurant - à l'exception de la photo, du numéro de RN et des empreintes digitales - peuvent être lues ou enregistrées conformément aux dispositions légales en matière de protection de la vie privée et des données à caractère personnel. Il est précisé que la photo et le numéro de RN ne peuvent être utilisés que moyennant autorisation légale ou par arrêté ministériel.

L'exposé des motifs précise que le législateur ne peut pas imposer la détermination des autorités habilitées à lire la photo de la carte d'identité - comme cela sera fait pour la lecture de l'image des empreintes digitales - et justifie sa position sur base du fait que la photo est visible à l'œil nu sur la carte d'identité.

Cette justification ne convainc pas. **Dans la mesure où la lecture automatisée et l'enregistrement de la photo de la carte d'identité génèrent un risque particulier en terme de fraude à l'identité ; l'Autorité considère que les autorités habilitées à procéder à de tels traitements devraient être déterminées limitativement par la loi et des mesures de protection techniques spécifiques devraient entourer la lecture automatisée de la photo de la carte d'identité.**

15. L'article 6 §4 al. 2 in fine en projet de la loi de 1991 conditionne la lecture et l'utilisation de la carte d'identité électronique à la nécessité d'obtenir préalablement le consentement libre spécifique et éclairé de son titulaire et l'alinéa 4 de cette même disposition prévoit que « *sans préjudice de l'article 1er de l'AR du 25/03/2003, le titulaire de la carte d'identité peut refuser que ses données soient lues/enregistrées sauf dans les situations déterminées par AR délibéré en conseil des ministres* ». **Le considérant 78 de l'avis de la CPVP n'a pas été suivi.** Le gouvernement fait une lecture de l'AR du 25 mars 2003 contraire de celle de la CPVP en considérant que cet AR s'applique aussi aux acteurs du secteur privé.

Or, l'Autorité rappelle que cet AR du 25 mars 2003 (et plus spécifiquement son article 1er) a été pris en exécution de l'article 6, §7 de la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité qui délègue au Roi le soin de déterminer « **les autorités et officiers publics sur réquisition desquels la carte d'identité doit être présentée** » ; ce qui conforte la position de la CPVP et sa remarque faite au cons.78 : contrairement à ce qui est relaté dans l'Exposé des motifs, cet AR n'est pas applicable au secteur privé.

Par conséquent, selon le libellé de l'article 6, §4 en projet de la loi de 1991, tous les acteurs du secteur privé devront demander le consentement préalable de la personne concernée pour lire ou utiliser la carte d'identité électronique d'une personne. **Cela risque fortement de mettre à mal les acteurs privés qui sont tenus par une obligation légale (antérieure au présent projet de loi) de collecter l'identité de personnes par le biais de leur carte d'identité**. Afin d'éviter cela, Il convient d'ajouter à la fin de l'alinéa 2 en projet de ce futur art. 6 , §4, « Sauf disposition légale contraire ».

De plus, en dehors des dispositions légales prévoyant la lecture de la carte d'identité, certains types de contrats (généralement les contrats synallagmatiques à prestations successives pour autant que cela soit nécessaire) peuvent nécessiter de s'assurer de l'identité correcte de la personne concernée au moment de leur conclusion et constituer une base légitime pour demander à une personne la présentation de sa carte d'identité. Or, en limitant l'option du consentement pour ce faire, cela risque également de mettre certains acteurs du secteur privé dans l'impossibilité de vérifier l'identité de leur cocontractant par ce biais. Il est **renvoyé à ce sujet à la Recommandation d'initiative 03/2011 de la CPVP** relative à la prise de copie des cartes d'identité ainsi qu'à leur utilisation et à leur lecture électronique.

16. **L'article 28** du projet de loi confère au Ministre de l'intérieur le pouvoir d'autoriser les **accès au Registre des cartes d'identité** mais ce faisant il étend **également les bénéficiaires potentiels desdites autorisations - qui sont actuellement limités aux autorité publiques - et ce, sans aucune justification**.

Dans la mesure où ces registres des cartes d'identité sont plus sensibles par rapport au Registre national en raison des données qu'ils contiennent et au vu du risque de fraude et de vol d'identité pouvant résulter d'une utilisation détournée de la photo de la carte d'identité, ces registres doivent bénéficier d'une accessibilité restreinte par rapport au Registre national. Un option logique serait de limiter leur accessibilité aux autorités compétentes à des fins de détections des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution des sanction pénales.

17. L'article 29 du projet de loi modifie l'article 6ter de la loi 1991 de manière telle qu'il n'est dorénavant plus prévu dans la loi que les fonctions électroniques des cartes d'identité volées ou perdues sont suspendues ou retirées directement par la Commune. La détermination de ces modalités est déléguée dorénavant au Roi. L'intérêt de déléguer cela au Roi n'apparait pas. Cela devrait être prévu dans la loi directement. Il importe que ces fonctions soient directement

suspendues en cas de vol ou perte.De plus, la délégation au Roi faite à l'article 6ter al.4 en projet comprend également la détermination des instances auprès desquelles ces déclarations de vol doivent être faites alors que l'alinéa 1 de l'article 6ter en projet le détermine déjà.

18. En ce qui concerne l'article 30 du projet de loi relatif à l'application **Checkdoc**, **l'avis de la Commission** - recommandant que les utilisateurs de cette application qui auront accès à des données à caractère personnel des citoyens (informations si oui ou non leur carte d'identité est encore valide) soient préalablement identifiés et authentifiés – **n'est pas suivi**.

L'exposé des motifs relève l'impossibilité d'identifier et/ou d'authentifier vu la nécessité d'accessibilité la plus large possible du service. Ce faisant, **les citoyens seront dans l'impossibilité de connaitre les destinataires de leurs données à caractère personnel** (information selon laquelle leur carte d'identité ou leur passeport est encore valide ou non – soit a été volé, est perdu ou périmé) **qui utilisent ce service checkdoc s'ils en font la demande d'accès** ; **ce qui ne peut être acceptable**.

De plus, la version de l'avant-projet de loi de cet article prévoyait que les services du Registre national conservent pendant 10 ans à partir de la date de la vérification des données relatives aux documents dont la validité a été vérifiée ainsi qu'aux utilisateurs de l'application informatique checkdoc. **Il importe que le projet de loi reprenne également cette précision par souci de prévisibilité vis-à-vis des utilisateurs de checkdoc**.

Si ces remarques ne sont pas suivies, il importe à tout le moins qu'une **évaluation des risques d'une telle ouverture de l'utilisation de cette application checkdoc** (risque de fraude à l'identité, falsification de documents d'identité…) soit faite préalablement et que l'option choisie fasse l'objet d'une justification sur base des conclusions de cette évaluation des risques.

19. **A propos de l'insertion des empreintes digitales de toute la population dans la puce électronique de la carte d'identité (art 27 projet de loi)**

---

20. Le projet de loi n'a pas remédié aux critiques émises à ce sujet par l'Autorité de protection des données dans son avis 18/2018 du 28 février 2018 (points 62 à 71).

21. Même s'il est prévu que les empreintes digitales seront uniquement conservées sur la puce de la carte d'identité, l'attention des parlementaires est spécifiquement attirée sur les points ci-après développés.

22. Contrairement à ce qui est repris dans l'Exposé des motifs, la Commission européenne n'a pas émis de recommandation sur l'insertion des empreintes digitales dans les cartes d'identité mais a uniquement déposé une **proposition de Règlement européen de la Commission européenne du 17 avril 2018** sur l'insertion de données biométriques dans les cartes d'identité européennes. Cette proposition de Règlement européen - qui contrairement au projet de loi belge actuellement en discussion précise tout de même explicitement de manière limitative les finalités pour lesquelles les données biométriques (image faciale et empreinte digitale) pourront être utilisées - a quant à elle fait l'objet d'un **avis très critique du contrôleur européen à la protection des données**[1] **et** doit encore poursuivre son processus législatif européen.

23. Il n'y a toujours **pas de réelle justification de la mesure envisagée** dans l'exposé des motifs alors que cela a été demandé par l'Autorité de protection des données. Notre carte d'identité est déjà dotée de dispositifs de lutte contre la falsification (hologramme, ...) ainsi que d'un élément biométrique (l'image faciale). **En quoi concrètement est-ce insuffisant ? Quelles sont les statistiques dont disposent le gouvernement qui étayent la mesure envisagée ?**

24. Dans son avis précité, le contrôleur européen à la protection des données (CEPD) a relevé que les **statistiques ne plaident pas en faveur de la proposition de la Commission européenne** qui va dans le même sens de celle du gouvernement. Des statistiques de l'agence européenne des gardes-frontières (frontex) ne révèlent qu'un constat de 38.870 cas d'utilisation frauduleuse de cartes d'identité nationale pour la période 2013-2017. De plus, on constate une baisse d'utilisation de titre de séjour frauduleux de personnes en provenance des pays tiers depuis 2015 de l'ordre d'au moins 11%.

---

[1] Avis 07/2018 du 10 août 2018 du CEPD sur la proposition de Règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents

25. **L'assimilation des cartes d'identité avec les passeports qui est avancée par le gouvernement pour justifier cette mesure n'est pas acceptable** : même si les cartes d'identité peuvent aussi être utilisées comme titre de voyage dans l'Union européenne, elles ne font actuellement pas l'objet de contrôle systématique pour ces voyages vu le principe de liberté de circulation au sein de l'Union européenne. De plus, contrairement aux passeports, les cartes d'identité nationale offrent beaucoup d'autres utilisations (applications du secteur privé, ...). Ce point a également été relevé par le CEPD dans son avis. **Compte tenu des différences entre les cartes d'identité et les passeports, l'introduction dans les cartes d'identité d'éléments de sécurité pouvant être considérés comme appropriés dans le cas des passeports ne peut être automatique, mais exige une réflexion et une analyse approfondie qui ne semble pas avoir été réalisée**.

26. **Aucune analyse préalable d'impact relative à la protection des données (DPIA) ne semble avoir été réalisée sur le projet d'insérer l'image des empreintes digitales des citoyens dans la puce de la carte d'identité électronique**. L'exposé des motifs précise simplement qu'un « DPIA sera (est) fait » « zullen worden uitgevoerd » dans la version néerlandaise.

    Or, la mesure envisagée doit faire l'objet d'un DPIA en vertu de l'article 35.2.b du GDPR et cela doit se faire préalablement à son encadrement légal étant donné qu'il est fort probable que le résultat de cette analyse conclue à l'adoption d'autres mesures ou, comme cela a été le cas pour l'analyse d'impact de la proposition de Règlement européen de la Commission européenne - à la limitation du caractère obligatoire de l'insertion de données biométriques dans les cartes d'identité à l'image faciale de leur porteur et la précision du seul caractère facultatif de l'insertion des empreintes digitales[2].

27. L'interdiction de traitement des données biométriques ne peut être levée que sur base de l'article **9.2.g du RGPD** qui exige non seulement le motif d'intérêt public important mais également notamment le **caractère proportionné de la mesure face à l'objectif poursuivi et l'adoption de mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts des personnes concernées**. **Elles sont actuellement insuffisantes** :

[2] Point 31 de l'avis 07/2018 du contrôleur européen sur cette proposition de Règlement «Après la comparaison des options stratégiques, l'analyse d'impact indique que l'option ID 1) est la plus appropriée pour promouvoir les objectifs de renforcement de la sécurité aux frontières et au sein des États membres, ainsi que la liberté de circulation. Il est à noter que l'option ID 1) privilégiée par le rapport d'analyse d'impact intégrerait une «puce RFID obligatoire contenant des données biométriques (image faciale obligatoire, empreintes digitales facultatives)» Autrement dit, l'option stratégique soutenue par l'analyse d'impact accompagnant la proposition inclurait les empreintes digitales de manière optionnelle, et non comme une condition obligatoire. » Même si la Commission européenne n'en a manifestement pas tenu compte dans sa proposition finale; ce qui est critiqué dans l'avis du CEPD (cf. infra).

a. Le choix du gouvernement de collecter et stocker dans la puce de la carte **l'image numérisée des empreintes digitales** ne constitue selon le CEPD pas un choix des plus opportun au vu du **risque d'usurpation d'identité** en cas de hacking des données figurant sur la puce électronique de la carte[3]. Il convient de revoir ce choix et de **limiter les données dactyloscopiques stockées dans la puce des cartes d'identité à un sous-ensemble de caractéristiques extrait de l'image de l'empreinte digitale ou encore à des techniques biométriques sans trace (contour de la main, réseau veineux d'un doigt…).**
b. Au lieu de déléguer au Roi la tâche de déterminer les autorités qui seront habilitées à lire les empreintes digitales, c'est au législateur au sens formel du terme qu'il appartient de le faire.
c. **Il convient également que la loi précise que la lecture de ces données ne pourra se faire que pour vérifier l'authenticité de la carte d'identité**. Il convient de prévoir déjà dans la loi des mesures de limitation pour les lecteurs de cartes qui permettront de lire les empreintes digitales.
d. **Quelles seront les mesures de protection spécifiques qui seront prises pour limiter au maximum le risque de hacking du certificat de la carte d'identité qui contiendra l'image des empreintes digitales que ce soit tant en terme de sécurisation de la puce dans laquelle ces données seront insérées que de sécurisation des lecteurs de ces données ?**
e. Quelles sont les **mesures de protection pour la base de données temporaire qui reprendra de manière centralisée les empreintes digitales pendant 3 mois et quel en sera le responsable de traitement ?**
f. Enfin, comme relevé par le CEPD, des **enfants de moins de 14 ans** ne devraient pas être soumis à cette mesure.

[3] Comme relevé par le CEPD dans son avis, "dans l'hypothèse d'une faille de sécurité, l'image des empreintes digitales stockée sur un document d'identité perdu ou volé pourrait être récupérée et utilisée de manière criminelle pour émettre un faux jeu d'empreintes digitales permettant d'usurper l'identité du titulaire de la carte ».

PAR CES MOTIFS,

Outre les remarques précitées, l'Autorité émet **un avis défavorable** sur le projet de loi principalement en raison de son article 27 qui prévoit l'insertion des empreintes digitales dans les puces électroniques des cartes d'identité.

Pour les motifs explicités dans la présent avis (points 19 et suivants), il est recommandé aux parlementaires de demander le retrait de cette mesure du projet de loi en raison de la nécessité et de l'obligation légale, prévue à l'article 35.3.b du RGPD, de procéder préalablement à l'analyse de son impact relative à la protection des données et de disposer de statistiques et d'éléments concrets justifiant le caractère insuffisant de notre modèle actuel de carte d'identité au regard de la lutte contre la falsification de carte d'identité dans la mesure où elle dispose déjà d'un élément biométrique (l'image faciale) et de dispositifs de lutte contre sa falsification (hologramme, …).

Au lieu d'anticiper la proposition de Règlement européen de la Commission européenne, il serait préférable d'attendre que cette proposition atteigne la fin de son processus législatif européen d'autant plus que ce projet a fait l'objet d'un avis très critique du Contrôleur européen à la protection des données (avis CEPD 07/2018 du 10 août 2018).

L'Administrateur f.f., Le Président

(sé) An Machtens (sé) Willem Debeuckelaere