Avis n° 57/2017 du 11 octobre 2017

Objet : Avis d'initiative relatif au projet de loi modifiant la loi du 15 décembre 1980 *sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers* et la loi du 12 janvier 2007 *sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers* (CO-A-2017-047)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 29 ;

Vu les informations complémentaires du Commissaire général aux réfugiés et aux apatrides, reçues le 29 août et le 5 septembre 2017 ;

Vu le rapport de Monsieur Willem Debeuckelaere ;

Émet, le 11 octobre 2017, l'avis suivant :

REMARQUE PRÉALABLE

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement général 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 la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016[1].

Le Règlement, couramment appelé RGPD (Règlement général sur la protection des données), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et est automatiquement applicable deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie que depuis le 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) de l'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

---

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

Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil*

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=OJ:L:2016:119:TOC.)

I. CONTEXTE DE LA DEMANDE D'AVIS

1. La Commission souhaite émettre un avis concernant le projet de loi *modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers*, ci-après l'avant-projet de loi.

2. Le projet de loi transpose différentes directives européennes en droit belge, dont la Directive 2013/32/UE du 26 juin 2013 (Directive 2013/32/UE), qui est importante dans le cadre du présent avis[1]. La transposition de cette directive a des conséquences sur les modalités de l'examen dans le cadre de la procédure d'asile. La Directive 2013/32/UE renvoie à l'application de la Directive 95/46/CE du 24 octobre 1995 relative au traitement de données à caractère personnel[2].

3. L'avis concerne spécifiquement l'article 10 du projet de loi qui remplacera l'actuel article 48/6 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers (la loi relative aux étrangers). Comme démontré ci-après, cette disposition concerne le traitement de données à caractère personnel de demandeurs d'asile, à savoir leur identité et ainsi que de nombreuses données qui concernent la vie privée. La LVP est donc d'application.

4. La Commission constate que le projet de loi a été adopté par la Commission de l'Intérieur, des Affaires générales et de la Fonction publique le 10 août 2017. La Commission rappelle l'article 29, § 1 de la LVP en vertu duquel la Commission, sur demande notamment du Gouvernement ou des Chambres législatives, émet des avis *sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre de la présente loi, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel*. La Commission n'a reçu aucune demande du Secrétaire d'État à l'Asile et la Migration au sujet du projet de loi.

5. Bien que la LVP n'impose pas la consultation de la Commission, elle attire l'attention, par pur souci d'exhaustivité, sur le fait que :

- l'article 28, deuxième alinéa, de la Directive 95/46/CE requiert la consultation de la Commission;

---

[1] Directive 2013/32/UE du parlement européen et du conseil du 26 juin 2013 *relative à des procédures communes pour l'octroi et le retrait de la protection internationale (refonte)*.

[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*.

- depuis l'entrée en vigueur du GDPR en date du 24 mai 2016, un avis *doit* être demandé en ce qui concerne les traitements de données à caractère personnel susceptibles d'engendrer un risque élevé pour les droits et libertés de personnes physiques.[3]

Le traitement de données à caractère personnel découlant de la modification législative évoquée ci-avant (contrôle du smartphone de demandeurs d'asile, de sa participation aux réseaux sociaux ou d'un autre support d'informations numériques) doit être qualifié de traitement susceptible d'engendrer un risque élevé[4].

II. EXAMEN DU PROJET DE LOI LIMITÉ À L'ARTICLE 10, § 1, QUATRIÈME ALINÉA

A. Considérations générales

6. L'article 10 du projet de loi adopté maintient le principe de l'obligation de coopération du demandeur d'asile. Cela implique que pendant la procédure d'asile, le demandeur d'asile doit apporter sa pleine coopération à l'examen. Au cours de l'examen, le demandeur d'asile a ainsi l'obligation, à l'égard du Commissaire général aux réfugiés et aux apatrides (CGRA), de présenter les faits et éléments pertinents sur la base desquels le CGRA peut prendre une décision au sujet de la demande de protection internationale.

7. Ces faits et éléments concernent notamment l'âge, le passé, l'identité, le sexe, la nationalité et les lieux de résidence du demandeur. L'obligation de coopération du demandeur d'asile consiste à ce que ce dernier remette la documentation et les documents utiles aux collaborateurs du CGRA afin que la demande d'asile puisse être examinée correctement (voir l'article 48/6 de la loi relative aux étrangers).

8. En ce qui concerne cette obligation de coopération, l'article 10, § 1, quatrième alinéa du projet de loi insère une nouveauté importante faisant l'objet du présent avis : "*Si les instances chargées de l'examen de la demande ont de bonnes raisons de penser que le demandeur retient des informations, pièces, documents ou autres éléments essentiels à une évaluation correcte de la demande, elles peuvent l'inviter à produire ces éléments sans délai, quel que soit leur support. Le refus du demandeur de produire ces éléments sans explication satisfaisante pourra constituer un indice de son refus de se soumettre à son obligation de coopération visée à l'alinéa 1er*".

9. Il ressort de l'article 10 du projet de loi que cette obligation de coopération concerne désormais aussi la fourniture de preuve par l'obtention d'un accès à des informations protégées sur des réseaux

[3] Bien que le RGPD ne puisse être imposé qu'à partir du 25 mai 2018.

[4] Voir les articles 57, alinéa 1, 36, alinéa 2 et 35 du RGPD.

sociaux, le smartphone, une clé USB, un CD-rom, une carte mémoire, etc. que le demandeur d'asile a sur lui. D'après l'Exposé des motifs, cela se fait sur la base du consentement du demandeur d'asile[5].

10. L'Exposé des motifs avance par ailleurs que le contrôle des systèmes informatiques et réseaux sociaux protégés est conforme à la LVP[6].

B. Quant au contrôle des systèmes d'information du demandeur d'asile

11. D'après les informations complémentaires fournies par le CGRA, l'accès à l'environnement numérique du demandeur d'asile ne peut être demandé que lorsque cela se révèle nécessaire pour permettre au CGRA d'évaluer la demande, et donc le besoin, de protection internationale. L'accès à l'environnement numérique sur le smartphone et/ou les réseaux sociaux protégés du demandeur d'asile pour fournir la preuve de son identité, de son origine et/ou du risque de persécution et la protection contre des violences de guerre ne peut donc pas se faire de manière systématique.

12. En outre, le (collaborateur du) CGRA n'a accès qu'à la partie privée des informations numériques du demandeur d'asile si ce dernier y *consent*. D'après le Secrétaire d'État à l'Asile et la Migration, il s'agit d'une pratique qui existe déjà[7], ce que confirment les informations complémentaires du CGRA : "*Dans la pratique, l'accès aux médias sociaux (par exemple la partie privée de Facebook) est donc demandé par les collaborateurs du CGRA lorsqu'il y a des indices selon lesquels la personne concernée dissimule certaines informations qui sont nécessaires à l'examen. Cela se fait dès lors dans un nombre limité de cas. Les informations sur d'autres supports d'information (gsm, pc portable, …) ne sont lues que si la personne concernée présente elle-même ces informations.*" [Traduction libre effectuée par le Secrétariat de la Commission vie privée, en l'absence de traduction officielle].

13. La Commission s'interroge quant à l'extension de cette mesure d'examen à l'autorité administrative. Sans vouloir créer une analogie avec le présent projet de loi, la Commission se réfère aux compétences de la police, par exemple, en matière de contrôle d'un smartphone[8] saisi ou à la

---

[5] Exposé des motifs du projet de loi, page 34. Rapport sur le projet de loi fait au nom de la Commission de l'Intérieur, des Affaires générales et de la Fonction publique par Madame Monica De Coninck, DOC. 54-2548/02, p.18.

[6] Exposé des motifs, page 36 : « *Cet alinéa est conforme à la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel du 8 décembre 1992 (M.B. 18 mars 1993).* »

[7] Rapport sur le projet de loi fait au nom de la Commission de l'Intérieur, des Affaires générales et de la Fonction publique par Madame Monica De Coninck, DOC. 54-2548/02, p.27.

[8] Art. 39bis Code d'instruction Criminelle (CIC)

§ 1 Sans préjudice des dispositions spécifiques de cet article, les règles de ce code relatives à la saisie, y compris l'article 28sexies, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique ou une partie de celui-ci.

§ 2. La recherche dans un système informatique ou une partie de celui-ci qui a été saisi, peut être décidée par un officier de police judiciaire.

Sans préjudice de l'alinéa 1er, le procureur du Roi peut ordonner une recherche dans un système informatique ou une partie de celui-ci qui peut être saisi par lui.

Les recherches visées aux alinéas 1er et 2 peuvent uniquement s'étendre aux données sauvegardées dans le système informatique qui est soit saisi, soit susceptible d'être saisi. A cet effet, chaque liaison externe de ce système informatique est empêchée avant que la recherche soit entamée.

§ 3. Le procureur du Roi peut étendre la recherche dans un système informatique ou une partie de celui-ci, entamée sur la base du paragraphe 2, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée:

- si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche; et

- si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès. En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues au paragraphe 6 s'appliquent.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le procureur du Roi communique sans délai cette information au Service public fédéral Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé.

En cas d'extrême urgence, le procureur du Roi peut ordonner verbalement l'extension de la recherche visée à l'alinéa 1er. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention des motifs de l'extrême urgence.

§ 4. Seul le juge d'instruction peut ordonner une recherche dans un système informatique ou une partie de celui-ci autre que les recherches visées aux paragraphes 2 et 3:

- si cette recherche est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche; et

- si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette recherche, des éléments de preuve soient perdus.

En cas d'extrême urgence, le juge d'instruction peut ordonner verbalement l'extension de la recherche visée à l'alinéa 1er. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention des motifs de l'extrême urgence.

§ 5. En vue de permettre les mesures visées à cet article, le procureur du Roi ou le juge d'instruction peut également, sans le consentement du propriétaire ou de son ayant droit, ou de l'utilisateur, ordonner, à tout moment:

- la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités;

- l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système.

Toutefois, seul le juge d'instruction peut ordonner cette suppression temporaire de protection ou cette installation de dispositifs techniques lorsque ceci est spécifiquement nécessaire pour l'application du paragraphe 3.

§ 6. Si des données stockées sont trouvées dans les systèmes informatiques concernés qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

En outre, les moyens techniques appropriés sont utilisés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Lorsque la mesure prévue à l'alinéa 1er n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes moeurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles ou, après en avoir pris copie, les retirer.

Il peut cependant, sauf dans le cas prévu à l'alinéa 4, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

En cas d'extrême urgence et s'il s'agit manifestement d'une infraction visée aux articles 137, § 3, 6°, 140bis ou 383bis, § 1er, du Code pénal, le procureur du Roi peut ordonner verbalement que tous les moyens appropriés soient utilisés pour rendre inaccessibles les données qui forment l'objet de l'infraction ou ont été produites par l'infraction et qui sont contraires à l'ordre public ou aux bonnes moeurs. Cet ordre est confirmé par écrit dans les meilleurs délais, avec mention des motifs de l'extrême urgence.

§ 7. Sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées, le procureur du Roi ou le juge d'instruction informe dans les plus brefs délais, le responsable du système informatique de la recherche dans le système informatique ou de son extension. Il lui communique le cas échéant un résumé des données qui ont été copiées, rendues inaccessibles ou retirées.

§ 8. Le procureur du Roi utilise les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données.

compétence d'inspecteurs sociaux d'accéder aux systèmes d'information en vue du contrôle du respect de la législation sociale. Dans les deux cas, la lecture de systèmes informatiques n'est permise que dans des circonstances spécifiques et si elle est entourée des garanties nécessaires. Ces conditions plus strictes sont imposées par le législateur parce que les informations contenues dans un smartphone et sur les réseaux sociaux protégés donnent une image très large et détaillée au sujet du (cœur-même) de la vie privée de l'utilisateur, et généralement aussi de celle de tiers. Le législateur fait ainsi savoir qu'il s'agit d'une ingérence profonde dans le droit à la vie privée à laquelle on ne peut recourir que dans des cas spécifiques, moyennant le respect de conditions légales.

14. Contrairement aux agents de police et aux inspecteurs sociaux, les collaborateurs du CGRA n'ont pas été formés pour exercer ces compétences étendues et ils n'ont pas non plus de tâches qui relèvent initialement de la législation pénale (spéciale). Si le collaborateur du CGRA venait à être confronté, lors de l'examen de la demande d'asile, à des indices d'infractions, il doit le signaler à le procureur du Roi en conformément à l'article 29 CIC.

C. Quant au consentement du demandeur d'asile

15. Il ressort de l'article 10, § 1, quatrième alinéa du projet de loi que le collaborateur du CGRA ne peut demander accès au support que lorsqu'il y a de "*bonnes raisons*" de penser que le demandeur d'asile "*retient*" des informations, pièces, documents ou autres éléments essentiels à une évaluation correcte de la demande d'asile. Il s'agit par exemple de lacunes dans les déclarations, d'incohérences ou de contradictions entre les informations fournies par le demandeur d'asile et d'autres informations disponibles[9]. L'accès aux communications privées du demandeur d'asile est donc purement basé sur la compétence d'appréciation du CGRA.

16. Le constat du collaborateur du CGRA, selon lequel le demandeur d'asile retient les informations utiles, peut donner lieu à ce qu'il soit demandé au demandeur d'asile de présenter les informations qui sont enregistrées dans un système informatique qu'il détient. Sans le consentement du demandeur d'asile, le collaborateur ne peut se procurer l'accès aux données qui sont enregistrées sur le support. La Commission fait à cet égard une distinction entre la situation où le demandeur d'asile présente de lui-même les informations au collaborateur du CGRA et celle où il est demandé au demandeur d'asile de donner accès aux systèmes d'information numériques qu'il détient ou aux informations privées sur des réseaux sociaux. Il est évident que l'article 10, § 1, quatrième alinéa vise uniquement cette

---

Des moyens techniques appropriés sont utilisés pour leur conservation au greffe.

La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents.

[9] Exposé des motifs, page 34-36.

dernière situation, étant donné qu'il est loisible à chacun de partager spontanément des informations numériques avec un tiers.

17. Dans la LVP, le "consentement" est défini comme étant : "*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*"[10]. Reste à savoir s'il est *de facto* question du consentement du demandeur d'asile, comme décrit ci-avant. En effet, on peut difficilement admettre que dans les circonstances données, le demandeur d'asile fournira son consentement[11] "librement[12]". En premier lieu, l'article 10, § 1, quatrième alinéa du projet dispose que le CGRA peut inviter le demandeur "*à produire ces éléments sans délai, quel que soit leur support*." La personne concernée se trouve donc dans une situation de soumission où la demande du collaborateur du CGRA d'accéder au smartphone ou aux informations privées de la page Facebook du demandeur d'asile sera rapidement considérée par ce dernier comme une injonction ou une obligation. Cette perception du demandeur d'asile sera encore renforcée du fait qu'il est communiqué au demandeur d'asile qu'à défaut d' "*explication satisfaisante*" de son refus de donner accès à ces systèmes d'information numériques, on considérera qu'il s'agit d'un manquement à l'obligation de coopération[13]. Et ce défaut de coopération peut être considéré comme un élément négatif dans l'examen de la demande de protection internationale[14]. Il en résulte que le consentement n'est pas dissocié de l'obligation de coopération dans le chef du demandeur d'asile.

D. Quant à l'accès aux systèmes informatiques du demandeur d'asile

18. De manière plus fondamentale, la Commission constate de graves lacunes quant à la qualité de l'article 10, § 1, quatrième alinéa du projet de loi. Lorsque les autorités portent atteinte à la vie privée en traitant des données à caractère personnel, des garanties doivent être prévues contre des mesures et décisions arbitraires. Ce n'est pas le cas en l'occurrence. L'article 10 du projet de loi ne répond pas aux questions suivantes :

---

[10] Article 1, § 8 de la LVP. À la lumière de la future application du RGPD, la Commission attire l'attention sur la définition du "consentement" qui n'est pas précisément concordante avec la définition de la LVP. Cela est dû notamment au fait que le Règlement tient compte du consentement dans l'environnement numérique. L'art. 4, 11) du RGPD décrit le consentement comme "*toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement*". Il ressort du considérant 32 de l'article 4, 11) du RGPD que le consentement peut être donné par le biais d'un acte positif clair posé par voie électronique. Le consentement réfléchi et univoque de la personne concernée doit ressortir de cet acte positif, basé sur des informations claires et spécifiques quant à la finalité pour laquelle le consentement est donné et à ses conséquences.

[11] Article 1, § 8 de la LVP : "*Par "consentement de la personne concernée", on entend toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*".

[13] Exposé des motifs, page 34-36.

[14] Ibid.

- De quelle manière l'accès au support d'informations numériques est-il donné ? Le collaborateur du CGRA recherche-t-il sur le support des informations pertinentes ou le demandeur d'asile garde-t-il le contrôle de son support afin de pouvoir donner accès lui-même à une sélection des informations ?
- De quelle manière les informations numériques obtenues sont-elles conservées ?
- - Conserve-t-on ou transcrit-on dans un rapport uniquement les informations pertinentes, ou le fait-on pour toutes les informations qui sont lues par le collaborateur du CGRA ?
- Qui traduit et interprète les informations fournies ?
- De quelle manière les informations numériques fournies sont-elles sécurisées et comment en garantit-on l'authenticité ?

19. La Commission constate qu'il manque un cadre légal suffisant concernant d'une part la manière dont l'accès au support numérique est réalisé et d'autre part les droits de la personne concernée. L'article 10, § 1, quatrième alinéa du projet dispose uniquement que lorsque le demandeur d'asile retient des informations, pièces, documents ou autres éléments essentiels à une évaluation correcte de la demande, le demandeur d'asile peut être invité à produire ces éléments «*sans délai*», quel que soit leur support. Le deuxième alinéa du paragraphe 2 de l'article 10 du projet de loi semble pouvoir concerner les informations numériques obtenues par le CGRA, mais il est rédigé de manière trop vague et dans des termes généraux, vu la nature de la mesure d'examen.

PAR CES MOTIFS,

la Commission émet un avis défavorable.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere