Avis n° 65/2019 du 27 février 2019

Objet: Demande d'avis relative à un projet d'accord de coopération modifiant l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative (CO-A-2019-014 + CO-A-2019-044)

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

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu le 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* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu la demande d'avis de la Vice-Présidente et Ministre de l'Action sociale, de la Santé, de l'Egalité des chances, de la Fonction publique et de la Simplification administrative du Gouvernement Wallon, Alda Greoli, reçue le 3 janvier 2019;

Vu la demande d'avis du Ministre du Budget, de la Fonction publique et de la Simplification administrative du Gouvernement de la Fédération Wallonie-Bruxelles, André Flahaut, reçue le 10 janvier 2019;

Vu le rapport de Debeuckelaere Willem et Verschuere Stefan;

Émet, le 27 février 2019, l'avis suivant :

I. OBJET DE LA DEMANDE ET CONTEXTE

1. La Vice-Présidente et Ministre de l'Action sociale, de la Santé, de l'Egalité des chances, de la Fonction publique et de la Simplification administrative du Gouvernement Wallon et le Ministre du Budget, de la Fonction publique et de la Simplification administrative du Gouvernement de la Fédération Wallonie-Bruxelles consultent l'Autorité pour avis à propos d'un projet d'accord de coopération modifiant l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative [**le projet**]. La Commission de la Protection de la Vie Privée s'est déjà prononcée dans ce contexte, lors du processus d'adoption de l'accord de coopération du 23 mai 2013[1].

2. Pour rappel, cet accord de coopération organise entre autorités publiques, le partage, via la Banque-Carrefour d'échange de données [**BCED**], de données provenant de sources authentiques de données et de banques de données issues de sources authentiques de données en Région wallonne et en Communauté française.

3. Des termes de la note rectificative au Gouvernement wallon, le projet a en substance pour objectif d'adapter le texte d'origine de l'accord de coopération afin que celui-ci corresponde mieux avec la réalité de terrain, de prendre en compte le RGPD et le droit belge y afférent, et de mettre en place une autorité de contrôle au sens du RGPD, à savoir la Commission Wallonie-Bruxelles de contrôle des échanges de données [**CCED**].

4. Remarques : l'Autorité a tout d'abord réalisé son analyse sur la base de la version coordonnée du texte où apparaissent les modifications apportées, version à laquelle est d'ailleurs relatif l'exposé des motifs et qui comporte des articles numérotés de 1 à 38. Ensuite, afin d'alléger le texte du présent avis, l'Autorité utilise en général les termes « sources authentiques de données » comme incluant les

[1] Avis de la Commission de la Protection de la Vie Privée n° 29/2012 du 12 septembre 2012.

« banques de données issues de sources authentiques de données », et procède à la distinction des concepts lorsque celle-ci est utile au propos.

II. EXAMEN DU PROJET

II.1. Principes de transparence et de légalité, et traitement ultérieur de données

II.1.1. Transparence et légalité

5. En vertu des principes de transparence et légalité consacrés dans les articles 8 de la CEDH et 22 de la Constitution, un décret doit prévoir clairement dans quelles circonstances un traitement de données à caractère personnel est autorisé[2], et en conséquence déterminer quelles sont les données traitées, les personnes concernées, les conditions et finalités dudit traitement, la durée de conservation des données[3] et les personnes y ayant accès[4]. L'Autorité a déjà eu l'occasion de rappeler ces principes[5]. Lorsque le fondement du traitement repose sur une base juridique de droit national, l'article 6, 3., du RGPD exige également spécifiquement que les finalités soient définies cette base.

6. Dans ce contexte, une délégation au Roi ou en l'occurrence, aux Gouvernements, « n'est pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur »[6].

7. Les principes juste exposés doivent être appliqués en prenant en compte la nature générale et abstraite du projet qui en substance, fixe un cadre pour l'échange en Wallonie entre autorités publiques de données à partir de sources authentiques de données en permettant une collecte unique auprès des citoyens et des entreprises, et pour le contrôle des traitements de données réalisés par ces autorités, sans prévoir directement des traitements de données particuliers (à quelques nuances près toutefois, voir *infra*, points n° 24). Ainsi, au-delà de cette finalité générale, le projet ne fixe pas lui-même les finalités déterminées et explicites des traitements des données provenant des sources authentiques, celles-ci ressortant d'autres textes le cas échéant futurs. Au regard des principes de transparence et de légalité, le projet appelle les commentaires suivants.

---

[2] En ce sens récemment, lire Cour constitutionnelle, arrêt n° 29/2018 du 15 mars 2018, points B.9 et s. et point B.13.3 en particulier.

[3] La Cour Constitutionnelle a admis que le « le législateur pouvait régler de manière générale les conditions de conservation des données à caractère personnel, ainsi que la durée de cette conservation », arrêt n° 29/2018 du 15 mars 2018, point B.23.

[4] Lire par exemple, Cour constitutionnelle, arrêt n° 29/2018 du 15 mars 2018, point B.18, et Cour Constitutionnelle, arrêt n° 44/2015 du 23 avril 2015, points B.36.1 et s.

[5] Voir Avis de l'APD n° 110/2018 du 17 octobre 2018, points 7-9.

[6] Voir Cour Constitutionnelle : arrêt n° 29/2010 du 18 mars 2010, point B.16.1 ; arrêt n° 39/2013 du 14 mars 2013, point B.8.1 ; arrêt n° 44/2015 du 23 avril 2015, point B.36.2 ; arrêt n° 107/2015 du 16 juillet 2015, point B.7 ; arrêt n° 108/2017 du 5 octobre 2017, point B.6.4 ; arrêt n° 29/2018 du 15 mars 2018, point B.13.1 ; arrêt n° 86/2018 du 5 juillet 2018, point B.7.2.

II.1.2. Généralisation du traitement ultérieur des données issues de sources authentiques

8. Le projet est conçu de manière telle qu'il organise le principe de la réutilisation des sources authentiques de données à d'autres finalités que celles pour lesquelles ces sources et banques de données ont été originellement mises en place. Ainsi, la labellisation implique que les données de la source authentique seront « communiquées à d'autres autorités publiques et réutilisées par celles-ci, à d'autres fins que celles qui étaient poursuivies par la collecte initiale » (article 4, paragraphe 1er, alinéa 1er, du projet), le projet entendant « réputer » « compatibles » de tels « traitements ultérieurs » (article 4, paragraphe 1er, alinéa 2). Et lorsqu'une donnée provenant de source authentique est mise à disposition par la BCED, « les autorités publiques sont obligées de passer par elle pour y accéder » (sauf exception) (article 6, paragraphe 1er, alinéa 1er, du projet). Une fois autorisée par la CCED à accéder à la donnée concernée, via la BCED, l'autorité publique en cause ne peut alors plus collecter la donnée auprès des citoyens, entreprises ou autres (article 8, paragraphe 1er, du projet).

9. L'article 6, 4., du RGPD prévoit trois hypothèses limitatives dans lesquelles des données peuvent être traitées ultérieurement à une fin autre que celle qui a justifié leur collecte : celle du consentement de la personne concernée, celle du traitement fondé sur le droit de l'Union ou le droit national (ou d'une entité fédérée) constituant une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, 1., du RGPD, et enfin, l'hypothèse dans laquelle le responsable du traitement *in casu*, évalue si le traitement ultérieur envisagé est compatible avec le traitement initial au regard d'une série d'éléments à prendre en compte (article 6, 4., points a) à e) du RGPD).

10. Le projet se rattache à la deuxième hypothèse en organisant par accord de coopération entre deux entités fédérées, la réutilisation des données issues de sources authentiques. Ce faisant, et d'ailleurs en tout état de cause, sauf à violer l'article 6, 4., du RGPD, il ne peut réputer automatiquement compatible les traitements ultérieurs qui seront fondés sur les règles du projet et les règles qui y sont liés (règles régissant la source authentique et règles régissant les missions de l'autorité publique qui entend accéder aux donnés). Juger du contraire priverait l'article 6, 4., alinéa 1er, de son effet utile. De plus, force est de constater que cette disposition en projet ne correspond pas aux critères de qualité requis explicités au point précédent. L'article 4, paragraphe 1er, alinéa 2, du projet doit être supprimé, et la validité de chaque traitement ultérieur devra être évaluée *in concreto*, à l'aune du cadre normatif applicable.

11. Le paragraphe 2 de l'article 4 du projet, prévoyant qu'un traitement ultérieur à des fins historiques, statistiques, scientifiques ou archivistiques dans l'intérêt public est réputé compatible

lorsqu'il est effectué conformément aux conditions fixées par le titre 5 de la LTD doit également être supprimé pour la même raison. La comptabilité d'un tel traitement découlera de l'applicabilité directe du RGPD (voir les articles 5, 1., b), et 89 du RGPD) et des dispositions de droit national l'exécutant, au terme d'une application au cas par cas.

II.1.3. Source authentique de données et qualité de la norme créant la source authentique de données

12. **Source authentique et banque de données issues de sources authentiques**. Le projet définit la source authentique de données comme la « base de données instituée en vertu d'un décret ou d'un arrêté du Gouvernement contenant des données ayant valeur unique, labellisée et mise à disposition des autorités publiques par la Banque Carrefour d'Echange de Données » (article 2, 1°). Il définit ensuite la banque de données issues de sources authentiques comme la « base de données instituée par une disposition décrétale, regroupant un ensemble de données issues notamment de sources authentiques destinées à être réutilisées par les autorités publiques après leur mise à disposition par la Banque-Carrefour d'échange de données » (article 2, 2°).

13. **Banque de données issues de sources authentiques**. L'Autorité s'interroge avant tout sur la création de banque de données issues de sources authentique. En effet tout d'abord, comme la Commission pour la Protection de la Vie Privée a pu le soutenir, l'Autorité est d'avis qu'en principe, la source authentique de données est unique et ne doit pas être dupliquée[7]. Pour une protection accrue de la vie privée des personnes concernées, la même Commission s'est également clairement positionnée en faveur de l'intégration de services plutôt que de l'intégration de données[8]. Autrement dit, pour ces raisons, le recours aux banques de données issues de sources authentiques devrait être exclu.

14. Cela est d'autant plus vrai que l'Autorité note qu'en l'état de la définition des concepts du projet (article 2, 1°, 2° et 5°), il est permis que les « sources authentiques » de la banque de données issues de sources authentiques proviennent de *sources authentiques externes* (par exemple, une base de données fédérale). Dans ce contexte, l'Autorité d'une part, s'interroge sur la compétence et partant la légitimité, d'une entité fédérée à dupliquer de la sorte une base de données créée et organisée par une autre entité non partie à l'accord de coopération. Une justification au cas par cas sera nécessaire sur ce point. En tout état de cause d'autre part, une telle duplication et la réutilisation ultérieure des données ne pourront se réaliser *que dans la mesure où l'autoriserait le cadre normatif applicable (dispositions d'exécution y comprises) à la source authentique externe concernée*.

---

[7] En ce sens, voir Avis de la Commission de la Protection de la Vie Privée n° 29/2012 du 12 septembre 2012, point n° 94, et lire Recommandation n° 09/2012 de la Commission de la Protection de la Vie Prive du 23 mai 2012, points nos 5, a. et c., 9 et 15.

[8] Recommandation de la Commission de la Protection de la Vie Privée n° 03/2009, points nos 5-12.

15. Par ailleurs, et sans préjudice du commentaire précédent, la lecture combinée des articles 1er et 2*bis* (définissant le gestionnaire de la banque de données issues de sources authentiques), 2, 6, 8, ainsi que 11 et 12 (relatifs à la BCED), ne permet pas de déterminer si une même donnée pourra être consultée via la BCED, à la fois à partir de sa source authentique et à partir d'une banque de données issues de sources authentiques au sein de laquelle elle se trouverait également. L'article 2, 2°*bis*, du projet spécifie toutefois que le gestionnaire de la banque de données issues de sources authentiques agit « pour le compte » de l'ensemble des sources authentiques. L'Autorité considère que le projet devrait clarifier ce point ainsi que les relations entre gestionnaire de source authentique et gestionnaire de banque de données issues de sources authentiques de données, gestionnaires au sujet desquels le projet se borne à définir des responsabilités propres. Il s'est dégagé, lors d'un échange avec les demandeurs au sein de l'Autorité, que les autorités publiques ne seraient obligées, par le projet, de réutiliser les données des banques de données issues de sources authentiques de données (plutôt que les sources authentiques elles-mêmes) que lorsque, au regard du traitement concerné, *l'ensemble* des types/catégories de données repris dans cette banque est nécessaire. Le projet doit être adapté en conséquence.

16. Enfin, le terme « notamment » repris dans la définition de la banque de données issues de sources authentiques devrait être omis dès lors que toute l'économie du projet repose sur la création et la réutilisation de sources authentiques de données (voir notamment l'article 1er du projet).

17. **Labellisation**. Ensuite, l'Autorité souligne que le projet ne prévoit pas de critères pour encadrer la labellisation (articles 4, paragraphe 1er, et 7, paragraphe 3, du projet) d'une base de données en une source authentique ou en une banque de données issues de sources authentiques, alors que tel devrait être le cas[9].

18. **Traitement ultérieur pour d'autres finalités**. Plus fondamentalement, il ressort clairement du projet que les données issues d'une source authentique pourront être traitées pour d'autres finalités et par d'autres autorités que celles qui étaient envisagées originellement lors de la création de cette source authentique. Autrement dit, le projet a pour objet et pour effet de permettre un traitement ultérieur par d'autres autorités publiques qui ni l'un, ni les autres, ne sont déterminés au moment de la création de la source authentique. Alors que tel devrait en principe être le cas au regard des principes de transparence et de légalité évoqués précédemment[10] (voir *supra*, points nos 5-6). Cette approche conçoit la source authentique comme pouvant évoluer par l'application des règles du projet et d'autres règles futures y combinées, règles qui pourront être consacrées formellement, dans d'autres textes que celui même qui consacre la source authentique de données.

[9] Dans ce domaine, lire par exemple Avis de la Commission de la Protection de la Vie Privée n° 02/2018 du 17 janvier 2018.

[10] Voir par exemple l'article 9 de la loi du 19 mai 2010 portant création de la Banque-Carrefour des véhicules.

19. L'Autorité est d'avis que le projet peut suivre cette approche que la Commission de la Protection de la Vie Privée a déjà acceptée dans son principe[11], pour autant que l'accord de coopération ne puisse constituer un blanc-seing pour contourner l'exigence de légalité consacrée dans l'article 22 de la Constitution : le projet ne peut permettre de manière générale et abstraite que des arrêtés du Gouvernement puissent *in fine*, régir des sources authentiques de données de leur création à leur réutilisation. En conséquence, l'Autorité est favorable à l'approche poursuivie par le projet sous réserve de ce qui suit, *lorsque les sources authentiques de données contiennent des données à caractère personnel* :

- premièrement, en application des principes de transparence et de légalité évoqués précédemment (voir *supra*, points nos 5-6), eu égard à la portée de l'accord de coopération, tant la source authentique de données que la banque de données issues de sources authentiques de données devraient être créées et organisées par un décret (voir les articles 2, 1° et 2°, et 7, paragraphes 1er, 2 et 3 du projet) ; ce qui n'empêche pas qu'un arrêté de Gouvernement puisse désigner, parmi les sources qui sont organisées via décret, lesquelles sont authentiques ;

- deuxièmement, toujours conformément à ces mêmes principes, les éléments essentiels des traitements de données ultérieurs devront également être déterminés par ou en vertu d'un décret. Autrement dit, les normes décrétales qui fonderont le traitement ultérieur de données issues de sources authentiques devront déterminer les éléments essentiels du traitement. Une fois de plus, un arrêté du Gouvernement ne pourra seul, en toute hypothèse, fonder le traitement ultérieur de la source authentique concernée, pour une finalité autre que celles ayant justifié sa création ;

- et troisièmement, dans le même sens que les deux commentaires précédents, l'Autorité souligne que les paragraphes 1er et 2 de l'article 7 du projet devraient également exiger des textes désignant les sources authentiques de données et banques de données issues de sources authentiques, la détermination des éléments essentiels du traitement, en ce compris les catégories de destinataires et finalités pour lesquelles ces derniers utiliseront les données.

20. **Collecte unique des données.** Enfin les paragraphes 1er des articles 6 et 8 du projet prévoient, du point de vue du citoyen et de l'entreprise, un principe de collecte unique des données conforme à la logique de l'e-gouvernement belge, lorsque les données sont mises à disposition via la BCED (voir encore l'article 12, paragraphe 2, du projet). La formulation de l'article 8, paragraphe 1er, doit toutefois être clarifiée en ce qu'elle prévoit que cette obligation est applicable « sauf si une exception de nature juridique ou technique rend impossible l'accès à ces données ». Juridiquement,

[11] Recommandation n° 09/2012 de la Commission de la Protection de la Vie Prive du 23 mai 2012, point n° 10.

l'hypothèse visée est-elle par exemple celle où une autorisation de la CCED serait remise en cause par une juridiction ? S'agit-il de viser d'autres règles qui empêcheraient la transmission des données et dans l'affirmative, lesquelles ? Le même commentaire vaut pour l'article 12, paragraphe 2, du projet.

II.1.4. Obligation de transparence particulière

21. Le projet consacre en son dispositif une série d'obligations de transparence spécifiques auxquelles l'Autorité est favorable. Ainsi, l'autorité publique qui demande des informations à des personnes devra indiquer le type de données qu'elles consultent à leur sujet, auprès de sources authentiques de données (article 8, paragraphe 1er, du projet), elles devront pré-remplir les demandes d'informations adressées aux personnes et indiquer l'origine des données (article 8, paragraphe 2, du projet), et les gestionnaires de sources authentiques de données devront mettre en place des moyens techniques offrant aux personnes concernées la possibilité, en substance, d'exercer certains de ses droits (consultation des données, rectification et identification des autorités publiques qui y ont accédé), du moins partiellement, par voie électronique, outre les obligations découlant du RGPD (article 9 du projet).

22. Si l'Autorité est favorable à ce dernier processus, c'est cependant sous réserve de ce qui suit. En effet, il ne constitue pas la mise en œuvre pure et simple du droit d'accès en application du RGPD, mais bien d'une mesure complémentaire. Ainsi, les moyens techniques électroniques en question permettront entre autres à la personne concernée « de connaître toutes les autorités publique qui ont, au cours des six mois écoulés, consulté ou mis à jour les données personnelles les concernant, à l'exception des autorités administratives et judiciaires chargées de la recherche et de la répression des délits ainsi que de la Sûreté de l'Etat et du Service général du Renseignement et de la Sécurité des Forces armées ». Indépendamment des questions de formulation (sont concernés les données « à caractère personnel » et probablement plus généralement, les autorités chargées de la recherche et de la répression des infractions), cette possibilité ouverte à la personne concernée est en effet plus limitée que le droit dont elle jouit au titre de l'article 15 du RGPD[12].

23. L'Autorité insiste dans ce contexte, sur l'importance d'informer correctement les personnes concernées sur le fait qu'il ne s'agit pas d'un outil leur permettant d'exercer leur droit d'accès au sens du RGPD, droit d'accès qui peut être exercé par ailleurs dans la portée qui lui est reconnue par le RGPD et le droit belge l'exécutant, et au sujet duquel elles devront être informées à partir de ces moyens techniques et électroniques, sauf à risquer de créer une confusion préjudiciable. De plus, l'Autorité considère que ce délai de 6 mois pourrait être étendu vu le champ d'application potentiel

[12] Voir également, sur le délai de conservation des informations relatives aux destinataires des données, CJCE, 7 mai 2009 (COLLEGE VAN BURGEMEESTER EN WETHOUDERS VAN ROTTERDAM c/ M.E.E. RIJKEBOER), aff. C-553/07.

très large et couvrant des autorités publiques ne rentrant pas nécessairement en contact direct avec les personnes concernées pour exercer leur mission de service public à leur égard.

II.1.5. Traitements particuliers découlant directement de l'accord de coopération

24. Le projet devrait encore déterminer les éléments essentiels des traitements de données qu'il est en mesure de prévoir directement (il en est ainsi des traitements qui seront réalisés par la CCED dans l'exercice de ses missions, voir *infra*, points nos 68 et s., ainsi que de certains traitements spécifiques dont semblerait être responsable la CCED, voir *infra*, point n° 115).

II.2. Répartition des compétences et autorités de contrôle

25. A titre préliminaire, l'Autorité rappelle que la question de la répartition des compétences en matière de vie privée et de protection des données relève *in fine* des compétences du Conseil d'Etat et de la Cour constitutionnelle. C'est au regard des jurisprudence de ces institutions qu'il incombera au demandeur de poser un choix clair, légal et cohérent dans l'exercice de sa compétence. L'Autorité ne peut que se borner d'une part, à constater qu'il est acquis que les entités fédérées sont compétentes pour créer des autorités de contrôle, ce que la Commission de la Protection de la Vie Privée avait déjà elle-même constaté : « À la lecture du considérant B.21 de l'arrêt n° 15/2008 du 14 février 2008 de la Cour constitutionnelle et au regard des compétences implicites visées à l'article10 de la loi spéciale [référence omise], la compétence des Régions et Communautés d'installer une autorité de contrôle de l'échange des données au sein de leur propre administration ne fait aucun doute »[13]. Et d'autre part, à s'interroger comme il suit.

II.2.1. Considérations de principe

26. La « Cour constitutionnelle et la section législation du Conseil d'Etat jugent désormais qu'il appartient […] à chaque législateur, dans la limite de ses compétences, de concrétiser les droits fondamentaux définis par des normes supérieures[…], dans les matières qui lui ont été attribuées[…] » (les références citées par le Conseil d'Etat sont omises)[14].

27. Pour ce qui concerne en l'occurrence l'ingérence dans la vie privée, ce n'est pas en application de l'article 10 de la loi spéciale de réformes institutionnelles du 8 août 1980 et au titre des compétences implicites (ou encore, de la réforme de l'Etat) que les entités fédérées sont compétentes, alors que le

[13] Avis de la Commission de la Protection de la Vie Privée n° 29/2012 du 12 septembre 2012, point n° 94.

[14] Avis du Conseil d'Etat n° 61.267/2/AV, du 27 juin 2017, point n° 3.

constituant l'avait envisagé[15], mais en vertu de la jurisprudence de la Cour constitutionnelle qui, dans une certaine mesure[16], partage l'objectif poursuivi par les pouvoirs implicites[17].

28. En matière de protection de la vie privée et des données, « [s]i les entités fédérées, chacune pour ce qui la concerne, adoptent des dispositions pour le traitement des données dans le cadre d'activités qui relèvent de leurs compétences – sachant que les articles 6, paragraphes 2 et 3, 9, paragraphe 4, du [RGPD] permettent l'adoption de dispositifs spécifiques –, elles sont habilitées à créer des autorités de contrôle de ces règles spécifiques »[18]. De la sorte, « à titre spécifique et complémentaire », des autorités de contrôle peuvent être créées « aux niveaux communautaire et régional dans le cadre des restrictions que les entités fédérées apportent au droit au respect de la vie privée »[19].

29. Cela étant, concernant l'ingérence dans le droit à la vie privée, la loi fédérale doit être prise en compte par les entités fédérées et constitue la règlementation minimale pour toute matière[20], ci-après [**le cadre minimal et général**]. Autrement dit, une entité fédérée ne pourra pas mettre en œuvre des règles moins protectrices des personnes concernées en matière de traitement de données à caractère personnel. La Cour constitutionnelle a pu juger par exemple que la « circonstance qu'une ingérence dans la vie privée soit la conséquence de la réglementation d'une matière déterminée attribuée au législateur décrétal n'affecte certes pas cette compétence, mais celui-ci est tenu de respecter la réglementation fédérale générale, qui a valeur de réglementation minimale pour toute matière. En ce que les dispositions attaquées visent l'échange de données personnelles, le législateur

---

[15] « *Un membre* résume le point de vue de la commission comme suit : 1° la 'mise en œuvre positive' du droit au respect de la vie privée et familiale relève, en vertu du deuxième alinéa de l'article 24*quater*, tant de la compétence des autorités fédérales que de celle des autorités communautaires ou régionales ; seul le législateur fédéral peut (par une loi) déroger au droit au respect de la vie privée et familiale (en vertu du premier alinéa de l'article 24*quater*), sous réserve des exceptions prévues par la loi spéciale de réformes institutionnelles, notamment en ce qui concerne les perquisitions (article 11 de la loi spéciale) et en ce qui concerne les compétences implicites (article 10 de la loi spéciale). Répondant à un membre, *le Premier ministre* confirme cette interprétation », *Doc. Parl.*, Chambre, 1993-1994, n° 1278/2, p., pp. 4-5.

[16] « Sans doute découle-t-il de l'article 22, alinéa 1er, de la Constitution que seul le législateur fédéral peut déterminer dans quels cas et à quelles conditions le droit au respect de la vie privée et familiale peut être limité, mais cette compétence ne peut raisonnablement concerner que les restrictions générales à ce droit, applicables dans n'importe quelle matière. *En juger autrement signifierait que certaines compétences des communautés et des régions seraient vidées de leur substance*. La circonstance qu'une ingérence dans la vie privée et familiale soit la conséquence de la réglementation d'une matière déterminée attribuée au législateur décrétal n'affecte pas la compétence de celui-ci » (italiques ajoutés par l'Autorité), Cour Constitutionnelle, arrêt n° 50/2003 du 30 avril 2003, point B.8.10.

[17] L'article 10 de la loi spéciale du 8 août 1980 de réformes institutionnelles tel qu'interprété par la Cour constitutionnelle permet aux entités fédérées, d'adopter une réglementation dans le domaine de compétence du législateur fédéral pour autant que trois conditions soient cumulativement remplies : cette réglementation est nécessaire à l'exercice de ses propres compétences par l'entité fédérée concernée, la matière en cause se prête à un régime différencié et enfin, l'incidence des dispositions envisagées par l'entité fédérée sur cette matière n'est que marginale. Voir notamment, Cour constitutionnelle : arrêt n° 78/2016 du 25 mai 2016, points B.9.2 et s. ; arrêt n° 152/2015 du 29 octobre 2015, point B.14.7 ; arrêt n° 105/2015 du 16 juillet 2015, point B.11 ; arrêt n° 29/2015 du 12 mars 2015, points B.11 et s. ; arrêt 74/2014 du 8 mai 2014, point B.9.6.

[18] Avis du Conseil d'Etat n° 61.267/2/AV, du 27 juin 2017, point n° 7.1.

[19] *Ibid.*, point n° C.

[20] *Ibid.*, points nos 4.2-5.

décrétal est lié par les garanties minimales prévues par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel »[21].

30. Le RGPD donne le pouvoir aux Etats membres de mettre en place une ou plusieurs autorités de contrôle (article 51, 1., du RGPD). Il en définit lui-même les caractéristiques, missions et pouvoirs (voir les articles 51 et s. du RGPD). Dans l'hypothèse d'une pluralité nationale d'autorités de contrôle, le RGPD prévoit d'une part, que l'Etat membre concerné doit désigner celle qui représente celles-ci au Comité européen de la protection des données (article 51, 3., du RGPD). L'article 116 de la LCA prévoit à cet égard que l'Autorité est le représentant commun des autorités de contrôle belges au sein de ce comité. D'autre part, il impose encore à cet Etat membre de définir le « mécanisme permettant de s'assurer du respect, par les autres autorités, des règles relatives au mécanisme de contrôle de la cohérence visé à l'article 63 » du RGPD (article 51, 3., du RGPD, voir également le considérant n° 119 du RGPD). En l'état du droit positif belge, un tel mécanisme n'existe pas. Dans l'hypothèse où des autorités de contrôle fédérales et d'entités fédérées coexisteraient, le Conseil d'Etat a rappelé la nécessité de conclure entre les différents niveaux de pouvoir, sur la base de l'article 92*bis* de la loi spéciale du 8 aout 1980, un accord de coopération au sujet des mécanismes de coopération prévus dans le RGPD.

31. En droit belge fédéral, l'article 4, paragraphe 1er, de la LCA prévoit que l'Autorité est responsable du contrôle des règles de protection des données dans le cadre de cette loi et des lois contenant des dispositions relatives à cette matière. Et en vertu de l'alinéa 2 de ce même paragraphe, l'Autorité exerce cette mission indépendamment du droit national applicable au traitement concerné, sur l'ensemble du territoire belge, sans préjudice des compétences des gouvernements et parlements des entités fédérées. Par ailleurs, l'Autorité est compétente lorsqu'aucune autre loi n'en dispose autrement (article 4, paragraphe 2, alinéa 2, de la LCA). D'un point de vue formel enfin, seul les LCA et LTD peuvent établir en droit fédéral, une autorité de contrôle au sens du RGPD.

32. A côté de l'Autorité, sont également autorités de contrôle fédérales, l'Organe de contrôle de l'information policière (voir l'article 4, paragraphe 2, alinéa 4, de la LCA), le Comité permanent R et le Comité permanent P (voir articles 95, 128, 161, 184 de la LTD).

II.2.2. Questions soulevées par ces considérations de principe

33. **Quelle compétence peut être attribuée à une autorité de contrôle d'une entité fédérée ?** Le pouvoir reconnu dans la position du Conseil d'Etat juste évoquée, des entités fédérées de créer des autorités chargées du contrôle des règles spécifiques qu'elles édictent dans le cadre des

[21] Cour Constitutionnelle, arrêt n° 15/2008 du 14 février 2008, point B.21, alinéa 2. Il ne s'agit que d'un exemple parmi d'autres décisions.

articles 6, 2. et 3., et 9, 4., du RGPD, soulève juridiquement et pratiquement, de l'avis de l'Autorité, les questions suivantes relatives à sa mise en œuvre.

34. **Compétence personnelle de contrôle**. Premièrement, le champ d'application *ratione personae* de cette compétence de contrôle doit-il être défini selon la qualité du responsable du traitement (une autorité publique instituée selon le droit de l'entité fédérée), un « critère organique », selon le fondement du traitement (un traitement nécessaire au respect d'une obligation légale de droit de l'entité fédérée ou nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique de l'entité fédérée, visé à l'article 6, 1., c) et e), du RGPD) que réalise ce responsable de traitement, un « critère de traitement », ou selon un cumul de ces critères organique et de traitement (à savoir, une autorité publique instituée selon le droit de l'entité fédérée qui réalise un traitement de données fondé dans le droit de l'entité fédérée) ? Sans doute le « critère organique » apparaît-il d'emblée plus praticable et sûr du point de vue de la sécurité juridique.

35. **Compétence matérielle de contrôle**. Deuxièmement, qu'en est-il du champ d'application *ratione materiae* de la compétence de contrôle : le contrôle serait-il limité aux seules spécificités et particularités consacrées dans le droit de l'entité fédérée dans la marge de manœuvre offerte par les articles 6, 2., et 9, 4., du RGPD, à l'exclusion du cadre minimal et général (voir *supra*, point n° 29), un « contrôle spécifique », ou s'étendrait-il, dans le domaine concerné, à l'ensemble des règles de protection des données applicable au traitement, un « contrôle global »)?

36. La réponse à ces questions dépend de l'interprétation à donner à l'article 22, alinéa 1er, de la Constitution, qui lui-même pose les questions suivantes.

37. **Quel pouvoir est compétent à l'égard de l'organisation du contrôle du cadre minimal et général visé à l'article 22, alinéa 1er, de la Constitution ?** Avant l'entrée en vigueur du RGPD, ce cadre minimal était composé de la loi du 8 décembre 1992 qui transposait les règles européennes antérieurement applicables au RGPD, en la matière, à savoir la directive n° 95/46[22] qui autrement dit, faisaient partie intégrante de ce cadre minimal. Il est logique que le pouvoir compétent pour ériger ce cadre minimal soit également celui qui est compétent pour en ériger une autorité de contrôle et ses pouvoirs. Le Conseil d'Etat a ainsi reconnu dans son avis précité qu'il « appartient à l'autorité fédérale, en vertu de sa compétence relative à la réglementation générale portant sur la limitation du droit au respect de la vie privée, d'édicter les règles concernant l'autorité de contrôle chargée de veiller au respect de cette réglementation générale »[23].

[22] Directive (CE) n° 95/46 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.

[23] *Ibid.*, point 6. Le Conseil d'Etat reconnaît bien que l'article 22 de la Constitution peut avoir pour effet que la création et l'organisation d'une autorité de protection des données exerçant ses missions en dehors des seules matières fédérales, peut relever de la compétence fédérale, voir les points 4.1 et s. de son avis.

38. La conséquence tout aussi logique d'une telle position, serait que l'exercice de cette compétence par les entités fédérées serait alors strictement limité par les conditions d'exercice des compétences implicites des entités fédérées (voir *supra*, la note de bas de page n° 17).

39. **Quelles règles relèvent du cadre minimal et général visé à l'article 22, alinéa 1er ?** Reste à déterminer quelles règles constituent ce cadre minimal et général. Car si les compétences sont bien exclusives, seul le pouvoir fédéral devrait organiser le contrôle en la matière. En droit positif, ce cadre devrait à tout le moins comprendre les LTD (qui notamment, exécute le RGPD et transpose la directive n° 2016/680[24]) et LCA.

40. Mais d'une part, cette assimilation ne va pas sans poser de questions : quelle spécialité peut revêtir ce cadre minimal et général ? Le titre 4 de la LTD vise par exemple le régime juridique applicable aux traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques visées à l'article 89, 2. et 3., du RGPD, lorsque le responsable du traitement entend déroger aux droits des personnes concernées. Et d'autre part, où se situe le RGPD par rapport à ce cadre minimal et général ? C'est à cette question que sont consacrés les développements suivants.

41. Comme la directive n° 95/46 transposée dans la loi du 8 décembre 1992 faisait partie du cadre minimal général, le **RGPD** devrait également être **considéré comme relevant de ce cadre minimal**. Dans le même sens, la loi fédérale n'est pas plus dissociée du RGPD que la loi du 8 décembre 1992 ne l'était de la directive n° 95/46, la première loi transposant la directive, la seconde exécutant le RGPD : quant aux règles dans leur aspect matériel, le fond minimum du droit reste le même. En l'occurrence alors, les entités fédérées resteraient libres, d'organiser le contrôle des règles spécifiques qu'elles édictent, conformément aux articles 6, 2. et 3., et 9, 4., du RGPD et *a priori,* finalement, aux autres règles laissant une marge de manœuvre aux Etats membre (l'article 23 par exemple, pourquoi exclure cet article des ingérences permises au niveau des entités fédérées ?), pour autant que ces règles relèvent bien de l'exercice de leurs compétences. Parmi ces règles, se trouveraient potentiellement les éléments essentiels des traitements de donnés devant être consacrés dans le décret afin d'assurer la conformité aux principes de transparence et de légalité consacrés dans l'article 22 de la Constitution (voir *supra*, points nos 5-6), et les spécificités adoptées au titre des articles 6, 2. et 3., 9, 4., du RGPD. Le pouvoir fédéral resterait compétent pour organiser le reste du contrôle à mettre en œuvre, à savoir celui des règles de protection des données au sujet desquelles le droit de

[24] Directive (UE) n° 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.

l'entité fédérée serait muet (par exemple, les obligations consacrées dans les articles 12 et s., dans la mesure où il n'y serait pas dérogé par ce droit de l'entité fédérée).

42. Cette position exclurait le « critère organique » de compétence de contrôle (puisqu'un responsable de traitement entité privée, est susceptible de réaliser un traitement de données en raison d'une obligation légale issue du droit d'une entité fédérée), répartirait les compétences selon un « critère de traitement », et fonderait les autorités de contrôle à un pouvoir de « contrôle spécifique » (voir *supra*, points 34-35). Le droit de l'entité fédérée et le registre des activités de traitement (article 30 du RGPD) contribueraient à identifier en pratique, l'autorité de contrôle compétente.

43. L'Autorité s'interroge toutefois sérieusement sur la praticabilité d'une telle solution qui impliquera, au regard d'un même traitement, des autorités de contrôle concurrentes dont la compétence serait répartie, sous l'angle de la protection des données, selon un critère relativement artificiel, et qui est de nature à générer de l'insécurité juridique et à nuire significativement à la transparence même du cadre normatif applicable à la protection des données, au préjudice des responsables de traitements et des personnes concernées. En effet, comment distinguer les règles spécifiques édictées par les entités fédérées des règles même du RGDP dont elles ne sont que la précision ou la dérogation encadrée, et auxquelles elles doivent être conformes ?

44. Ce dernier aspect de conformité soulève un problème additionnel. En effet, la consécration d'un cadre « minimal » implique inévitablement une hiérarchisation (partielle) entre les règles, celles du cadre spécifique ne pouvant se départir du cadre général (sauf à être plus protectrices). Or cette hiérarchisation ne pourrait se prolonger sous l'angle de la compétence de contrôle, sauf à mettre en place des autorités de contrôle qui ne seraient plus indépendantes et qui *in concreto*, auraient un pouvoir contraignant concurrent vis-à-vis d'un même traitement du point de vue du responsable du traitement (ainsi la règle générale du RGPD spécifiée par une entité fédérée dans le cadre d'un traitement constitue pour lui un même commandement), alors que leurs compétences devraient être exclusives. Le risque de décisions contradictoires créerait une insécurité préjudiciable aux responsables de traitements et personnes concernées.

45. Une alternative serait alors de considérer que le RGPD **ne relève pas de ce cadre minimal** et général *fédéral,* et qu'il constitue un cadre européen autonome. Seules les dispositions consacrées dans les LTD et LCA resteraient alors le cadre minimal et général à prendre en compte par les entités fédérées en vertu de l'article 22, alinéa 1er, de la Constitution. Et lorsque les entités fédérées agiraient dans le cadre de leurs compétences pour adopter des règles dans les hypothèses prévues aux articles 6, 2. et 3., et 9, 4., du RGPD, elle seraient également légitimes à établir des autorités de contrôles chargées de veiller à la conformité au RGPD en général, dans ces hypothèses.

46. De nouveau, le « critère organique » serait exclu mais dans cette hypothèse, les autorités des entités fédérées auraient un pouvoir de « contrôle global » (voir *supra*, points 34-35). Si cette solution paraît plus praticable, elle semblerait néanmoins significativement réduire la portée de l'article 22, alinéa 1er, de la Constitution pour ce qui concerne l'applicabilité du RGPD, si elle ne porte pas en elle la possibilité de lui ôter tout effet au regard des règles adoptées par les entités fédérées : que reste-t-il en effet du cadre minimal et général fédéral qui s'impose aux entités fédérées et dont le contrôle revient au pouvoir fédéral (l'organisation des voies de recours ? La détermination des sanctions aux violations des règles de protection des données – voir *infra* à ce sujet, point n° 66 - ?). Cette solution reste aussi porteuse d'insécurité juridique. Certes, c'est à moindre raison que la solution précédente, puisqu'il ne serait plus nécessaire de distinguer le contrôle selon les règles de protections des données. Mais il n'empêche, il est risqué de considérer qu'*a priori*, tout activité de traitement concernée pourra aisément être indentifiable et faire l'objet d'un traitement distinct, selon son fondement. Et enfin, le risque de décisions contradictoires d'autorités de contrôles concurrentes juste évoqué demeure, puisque demeure un cadre minimal et général, restreint toutefois. Bref la sécurité juridique est de nouveau mise à mal du point de vue des responsables de traitements et des personnes concernées.

47. Elle le serait encore plus par le recours au « critère organique ». En effet, les mêmes dispositions du droit d'une entité fédérée peuvent comporter deux facettes. D'un côté, elles fonderont la mission d'intérêt public de l'administration concernée et justifieront la nécessité pour celle-ci, de traiter des données à caractère personnel (article 6, 1., e), du RGPD). Et d'un autre côté, elles pourront nécessiter d'un responsable de traitement personne privée qu'il traite des données à caractère personnel afin de remplir les obligations que ces dispositions consacrent à son égard. Autrement dit de nouveau, des divergences d'opinions entre autorités de contrôle pourraient soumettre un même responsable de traitement à des impératifs contradictoires : d'un côté, ceux résultant du droit de l'entité fédérée jugé conforme aux règles de protection des données par l'autorité de contrôle de cette entité, de l'autre, ceux résultant des règles de protection des données interprétées autrement, par l'autorité de contrôle fédérale.

48. Finalement, à supposer que le « critère de traitement » puisse s'appliquer sans difficulté, *quod non*, lorsque le RGPD est exclu du cadre minimal et général (voir *supra*, points nos 45-46), le même responsable du traitement pourrait être soumis, en Belgique, à des interprétations différentes du RGPD selon les traitements qu'il réalise.

49. **Conclusion**. En conclusion, les développements précédents illustrent qu'il existe en l'état du droit belge, une incertitude dommageable concernant la portée des règles répartitrices de compétences au regard de la création, à différents niveaux de pouvoirs, de plusieurs autorités de contrôle et de l'organisation de leurs compétences. Même si c'est à bon droit que le demandeur revendique la compétence de créer une autorité de contrôle au sens du RGPD, la portée de sa

compétence doit être clarifiée par le Conseil d'Etat, la Cour constitutionnelle et un accord de coopération conclu par les législateurs (voir à tout le moins *supra*, point n° 30), sauf à créer une insécurité juridique susceptible de nuire considérablement à l'effectivité des règles de protection des données, au préjudice des responsables de traitement et des personnes concernées.

II.2.3. Application au projet

50. Sous réserve des questions développées précédemment concernant la répartition des compétence, il incombe en tout état de cause au demandeur de réaliser, dans la création et l'organisation d'une autorité de contrôle, des choix cohérents et conformes au RGPD. En l'occurrence, le projet transforme la Commission Wallonie-Bruxelles de contrôle des échanges de données [**CCED**] en autorité de contrôle au sens du RGPD. A cet égard, l'Autorité émet les considérations suivantes.

Compétence

51. **Autorités publiques.** La compétence de la CCED doit ressortir clairement du projet. L'article 3 du projet doit être adapté afin de tenir compte de la compétence telle que délimitée à l'article 22, paragraphe 1er, alinéa 3, du projet (voir également l'article 3, 6°, du projet, définissant la CCED) : la CCED « est chargée de contrôler, l'application de la réglementation relative à la protection des données à caractère personnel par les autorités publiques en Région Wallonne et en Communauté Française ». Le demandeur choisit par conséquent un « critère organique » de compétence (au sujet de ce critère, voir *supra*, points nos 34, 42, 46 et 47), celui des « autorités publiques ».

52. L'exposé des motifs du projet précise que la « définition d'autorité publique est reprise d'autres législations afin d'éviter des erreurs d'interprétation ». Selon le dispositif du projet, il s'agit de « a) les services des Gouvernements ; b) les pouvoirs locaux présents sur le territoire de la Région wallonne ; c) les organismes de droit public et personnes, quelles que soient leur forme et leur nature qui : i ont été créées pour satisfaire spécifiquement [des] besoins d'intérêt général ayant un caractère autre qu'industriel ou commercial et ; ii sont dotés d'une personnalité juridique et ; iii dépendent des Gouvernements ou des pouvoirs locaux relevant du présent point b), de l'une des manières suivantes : - soit leurs activités sont financées majoritairement par les Gouvernements ou les pouvoirs locaux relevant du présent point b) ; - soit leur gestion est soumise à un contrôle des Gouvernements ou des pouvoirs locaux relevant du présent point b) ; - soit plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par les Gouvernements ou les pouvoirs locaux relevant du présent point b) ; d) les associations formées par une ou plusieurs entités visées au a ; b ou c ». Cette définition est ainsi inspirée de la définition du concept de « pouvoir adjudicateur » tel que défini dans l'article 2, 1°, de la loi du 17 juin 2016 relative aux marchés publics (voir également l'article 5 de la LTD).

53. La définition retenue appelle deux commentaires. Premièrement, dès lors que le concept d'autorité publique est défini par l'article 2, 8°, du projet et y est délimité au regard de la compétence de la Communauté française et de la Région wallonne, les termes « en Région Wallonne et en Communauté Française doivent être supprimés de l'article 22, paragraphe 1er, alinéa 3 du projet. Deuxièmement, le concept de responsable du traitement n'exclut clairement pas que la Région wallonne et la Communauté française notamment, puissent elles-mêmes être considérées comme des responsables du traitement (sur ce concept, voir *infra*, points nos 88-90). La définition du concept d'autorité publique doit par conséquent être adaptée.

54. **Sphère de compétence de la CCED.** Le projet doit encore être cohérent au regard du choix posé quant à la sphère de compétence de la CCED, et en intégrer les conséquences juridiques. Ainsi, c'est dans l'intégralité de cette sphère de compétence que la CCED pourra, et le cas échéant devra, exercer les missions et pouvoirs lui incombant en application du RGPD (voir *infra*, points nos 73 et 75).

55. **Collaboration avec les autres autorités de contrôle.** L'article 26, qui régit la concertation et la collaboration de la CCED avec les autres autorités de contrôle devrait être clarifié. En vertu de celui-ci, le président de la CCED « veille à la compatibilité » des « recommandations et avis » de la CCED avec les « décisions » de l'Autorité, et des autorités de contrôle des autres entités fédérées. Quelle est la portée de cette obligation (s'agit-il d'une obligation de motivation des recommandations et avis qui divergeraient de ceux des autres autorités de contrôle ?) ?

56. Le président peut encore différer l'adoption d'un avis ou d'une recommandation afin de soumettre le dossier à l'avis préalable de l'Autorité. Or c'est à la LCA qu'il incombe de définir les compétences de l'Autorité (sur la compétence d'avis et de recommandation de l'Autorité, voir l'article 23 de la LCA). En tout état de cause, le délai imposé à l'Autorité ne devrait courir qu'à partir du moment où elle disposerait de tous les éléments nécessaires pour prendre position, et ceux-ci devraient comprendre le projet de recommandation ou d'avis de la CCED s'agissant de son domaine exclusif de compétence. C'est encore systématiquement, que la CCED devrait motiver les raisons pour lesquelles elle ne suivrait pas, en tout ou en partie, la position subséquente de l'Autorité.

57. L'Autorité est enfin d'avis que les règles de collaborations entre autorités belges devraient être adoptées dans un accord de coopération conclu entre l'Etat fédéral et les entités fédérées.

58. **Délégation des pouvoirs d'investigation**. L'article 28 du projet prévoit que la CCED peut « déléguer » le « pouvoir d'investigation tel que visé à l'article 58 du RGPD » (c'est en son 1., que l'article 58 du RGPD vise plusieurs pouvoirs d'enquête ; et c'est à ces pouvoirs, plutôt qu'à « cette

compétence », que doit faire référence l'alinéa 3 de l'article 28 du projet), « à un autre service ou à une autre autorité de contrôle en concluant un accord de collaboration ». Premièrement, l'Autorité s'interroge sur la légalité d'un tel pouvoir de délégation au regard du droit belge (notamment, le délégataire est en principe subordonné hiérarchiquement), question qui ne relève pas de sa compétence. Deuxièmement, l'Autorité est d'avis que de tels pouvoirs ne pourraient en toute hypothèse, qu'être exercés conformément au RGPD. Or ces pouvoirs ne peuvent être que ceux d'une autorité de contrôle au sens du RGPD. Par conséquent, les termes « à un autre service » doivent être supprimés. Nb : il s'est dégagé, lors d'un échange avec les demandeurs au sein de l'Autorité, que l'objectif de la disposition était plutôt de permettre une collaboration entre autorités. Le projet doit être adapté en ce sens.

Indépendance

59. **Concept d'indépendance**. La CCED doit exercer en toute indépendance les missions et pouvoirs dont elle est investie, conformément à l'article 52 du RGPD. Cette indépendance est un concept de droit européen[25] au regard duquel l'article 22, paragraphe 1er, alinéa 2, du projet n'apporte pas de plus-value. Au contraire, il peut sembler restrictif. Il convient de le supprimer.

60. **Conditions applicables aux membres**. Concernant les **conditions applicables à ses membres**, l'Autorité constate que la rédaction de l'article 22/1, paragraphe 4, n'est pas finalisée. Par ailleurs, l'Autorité ne voit pas pourquoi l'incompatibilité visée au 7° de ce paragraphe ne vise pas également la source authentique externe, comme le 8° vise d'ailleurs également les intégrateurs de service d'autres niveaux de pouvoir. L'Autorité recommande par ailleurs d'intégrer une incompatibilité similaire à celle consacrée dans l'article 38, 6°, de la LCA (« ne pas être mandataire d'une fonction publique », en l'occurrence à tout le moins, au sein d'une autorité publique relevant de la compétence de la CCED). La condition d' « être parfaitement compétents dans le domaine » visée au 6° toujours du même paragraphe, devrait être reformulée et semble à situer ailleurs dans ce paragraphe (le 6° vise les garanties d'indépendance et pas la compétence technique dans le domaine).

61. En matière de conflits d'intérêts, l'article 22/2, paragraphe 5, du projet, devrait être adapté à la lumière de l'article 43, alinéa 2, de la LCA, de manière telle que soient également pris en compte les intérêts personnel ou direct des parents ou alliés du membre jusqu'au troisième degré. Conformément à l'article 54, 1., f), du RGPD, le projet doit encore régler les interdictions d'activités, d'emplois et d'avantages incompatibles avec leurs obligations, « y compris après la fin de leur mandat ».

[25] Voir la jurisprudence de la Cour de justice en la matière, à savoir arrêt (Gr. Ch.) du 9 mars 2010 (COMMISSION c/ REPUBLIQUE FEDERALE D'ALLEMAGNE), aff. C-518/07 ; arrêt (Gr. Ch.) du 16 octobre 2012 (COMMISSION c/ REPUBLIQUE D'AUTRICHE), aff. C-614/2010 ; arrêt (Gr. Ch.) du 8 avril 2014 (COMMISSION c/ HONGRIE), aff. C-288/12.

62. **Représentant de la BCED.** L'article 22/4, alinéa 2, du projet prévoit qu'un représentant de la BCED participe sans voix délibérative à chaque réunion de la CCED, « afin d'assurer une collaboration et une coordination efficiente entre l'intégrateur de service et l'autorité de contrôle ». La BCED est un responsable de traitement autorité publique parmi d'autres, qui relève de la compétence de la CCED. Si l'Autorité perçoit l'objectif poursuivi par le demandeur, afin de sauvegarder l'indépendance de la CCED, celle-ci devrait avoir la faculté d'inviter au cas par cas, à tout ou partie de sa réunion, un représentant de la BCED afin que celui-ci réponde à ses éventuelles obligations. Lui imposer une telle présence systématique n'est pas conforme à l'indépendance dont elle doit jouir en application du RGPD. Cela étant, ceci ne s'oppose pas à ce qu'un représentant de la BCED puisse être présent lorsque la CCED exerce sa compétence d'autorisation des flux de données (voir *infra*, point n° 69), contexte dans lequel ce représentant peut apporter une expertise technique utile. Ce dispositif doit par ailleurs encore être articulé et coordonné avec l'obligation de confidentialité consacrée dans l'article 22/2, paragraphe 6, du projet.

63. **Personnel et budget propres, ressources humaines nécessaires.** L'article 52, 5., du RGPD, prévoit que chaque autorité de contrôle doit pouvoir choisir et disposer de ses propres agents, qui sont placés sous les ordres exclusifs de ses membres. L'article 52, 6., du RGPD prévoit encore notamment, qu'une autorité doit disposer d'un budget annuel public propre. L'article 22/3, paragraphe 2, alinéa 2, n'est pas conforme à ces dispositions du RGDP en ce qu'il prévoit que durant la période d'installation du secrétariat, la CCED peut s'adjoindre pour une période d'un an au plus, l'appui de la BCED dans la gestion de ses dossiers.

64. L'article 52, 4., du RGPD précise en outre qu'une autorité de contrôle doit notamment disposer des ressources humaines nécessaires à l'exercice effectif de ses fonctions. Eu égard aux compétences de la CCED, et en particulier à ses obligations en matière d'autorisation, l'Autorité émet des doutes quant à l'efficacité à cet égard, de l'article 22/3, paragraphe 2, alinéa 1er, qui prévoit que le secrétariat est « composé d'au moins trois personnes : une personne assurant la gestion administrative, une personne ayant des compétences juridiques approfondies en matière de protection des données, et une personne ayant des compétences informatiques approfondies en matière de sécurité de l'information ». Par ailleurs, le projet semble muet quant au statut de ces agents, et il ne définit pas non plus le lieu d'établissement de la CCED.

Missions et pouvoirs

65. L'article 23, alinéa 1er, du projet, prévoit que la CCED exerce l'ensemble des compétences (missions, selon les termes du RGPD) et pouvoirs visés aux articles 57 et 58 du RGPD.

66. **Amendes administratives**. Parmi d'autres mesures correctrices, l'article 58, 2., i), vise le pouvoir d'imposer des amendes administratives. L'article 221, paragraphe 2 de la LTD prévoit toutefois que l'article 83 du RGPD ne s'applique pas aux autorités publiques et leurs préposés ou mandataires sauf s'il s'agit de personnes morales de droit public qui offrent des biens ou des services sur un marché. L'article 5 de la LTD définit le concept d'autorité publique qui comprend notamment les entités fédérées et les autorités locales. L'Autorité comprend des termes du projet qu'il est dérogé à l'article 221 de la LTD, à supposer que cela soit conforme au regard des règles répartitrices de compétences, en octroyant à la CCED le pouvoir d'imposer des amendes administratives. L'Autorité invite cependant les demandeurs à clarifier leur intention à ce sujet.

67. **Contrôle de la BCED.** L'alinéa 2 de l'article 23 du projet, qui prévoit que la CCED est autorité de contrôle de la BCED, est superflu au regard du RGPD et des articles 3 et 22, paragraphe 1er, alinéa 3, du projet (sur les responsabilités au regard des traitements, voir *infra*, points nos 85 et s.). Il doit être supprimé.

68. **Compétence d'autorisation.** La CCED dispose d'un large pouvoir d'autorisation. Ainsi, elle doit autoriser « la diffusion des données à caractère personnel qui ont vocation à être diffusées largement » (article 18, alinéa 2, du projet) et plus généralement, tout accès à des données à caractère personnel issues d'une source authentique de données ou d'une banque de données issues de sources authentiques requiert une autorisation de la CCED (qui se prononce dans les soixante jours de la réception de la demande) (article 24/1 du projet).

69. L'article 36, 5., du RGPD permet une telle approche. Cependant, celle-ci s'éloigne significativement de l'approche fondée sur le risque et suivie par le GDPR globalement, et pourrait s'avérer en pratique, disproportionnée et assorties d'effets indésirables. Soumettre tout accès à autorisation risque de noyer dans la masse des flux, les traitements plus risqués et nécessitant une analyse plus approfondie. L'Autorité rappelle l'approche globale suivie par la LTD en la matière qui consiste en principe, à encadrer les flux entre administrations par des protocoles (voir l'article 20 de la LTD), seuls des domaines particuliers conservant d'une manière ou d'une autre, un régime d'autorisations préalables et ce toutefois, *par des entités qui ne sont pas des autorités de contrôle au sens du RGPD*[26]. L'Autorité est d'avis qu'une si large compétence d'autorisation entraîne une confusion entre le rôle d'une autorité de contrôle et celui d'un responsable du traitement ou le cas échéant, d'une entité instituée au titre de l'*accountability.* La réalisation d'une distinction entre l'autorité de contrôle et une entité instituée au titre de l'*accountability*, contrairement à ce qui est proposé dans le

[26] Sont concernés la Banque Carrefour de la Sécurité Sociale et le Registre National, voir les modifications apportées par la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du RGPD, et la loi du 8 août 1983 organisant un registre national des personnes physiques, telle que dernièrement modifiée par la loi du 25 novembre 2018 portant des dispositions diverses concernant le Registre national et les registres de population.

projet, permettrait d'ailleurs à l'intégrateur de services de mieux jouer son rôle dans le cadre des flux de données et de leur autorisation.

70. De plus, outre le fait le système d'autorisation envisagé se concentre sur des flux de données qui ne présentent pas nécessairement des risques élevés pour les droits et libertés des personnes concernées, l'Autorité relève le caractère potentiellement redondant du système envisagé d'autorisation avec l'obligation de réaliser un analyse d'impact relative à la protection des données prévue à l'article 35 du RGPD ainsi qu'avec les régimes d'autorisation précités. Une coordination doit être assurée et se refléter dans le projet.

71. Enfin sur le pouvoir des gouvernements de déterminer conjointement les conditions d'application de la compétence de la CCED de suspendre ou retirer une autorisation (article 24/1, paragraphe 4, du projet), l'Autorité rappelle que celui-ci sera en tout état de cause sans préjudice des pouvoirs dont disposera la CCED en vertu de l'article 58 du RGPD (en particulier, voir l'article 58, 2., f), du RGPD).

72. **Compétence d'avis.** Dans le prolongement de cette compétence d'autorisation, au sujet de la compétence d'avis de la CCED, cette dernière doit systématiquement rendre un avis préalable concernant les échanges de données à caractère personnel entre autorités publiques lorsque ces données ne sont pas issues de sources authentiques de données ou de banques de données issues de sources authentiques (article 24/1, paragraphe 2, du RGPD). L'Autorité renvoie à ce sujet au commentaire qui vient d'être réalisé au sujet d'une approche fondée sur le risque engendré par les traitements. Nb : le renvoi à la procédure visée à l'article 30, paragraphe 1er, du projet doit être adapté (probablement s'agit-il d'un renvoi au paragraphe 1er du même article).

73. Pour le surplus, le projet prévoit que la CCED « […] émet des avis sur la protection des données à caractère personnel *dans le cadre du présent accord et de ses dispositions d'exécution* » (italiques ajoutés par l'Autorité) (article 24, paragraphe 1er, alinéa 1er, du projet). Cette règle, qui impliquerait que pour le surplus (les autres textes normatifs pertinents en matière de traitement de données à caractère personnel), l'Autorité resterait compétente, n'est pas conforme au RGPD, aux règles répartitrices des compétences et au projet qui lus de manière combinée, imposent que la CCED puisse (ou doive, selon le cas) exercer sa compétence d'avis à l'égard des questions relatives *à l'ensemble des traitements de données relevant de sa compétence*. L'Autorité renvoie à cet égard *supra*, aux points nos 25 et s., à l'article 22, paragraphe 1er, alinéa 3, du projet, et surtout, aux article 36, 4., et 58, 3., b), du RGPD. Le projet, indûment restrictif, doit être adapté en conséquence. Pour la même raison, l'article 24, paragraphe 2, doit également être adapté : les mots « dans le cadre du présent accord et de ses dispositions d'exécution » doivent être supprimés.

74. L'article 7, paragraphe 3, du projet, qui prévoit, en toute hypothèse, que l'avis de la CCED ne doit pas être obtenu à propos d'un décret ou d'un arrêté désignant une source authentique, si cet avis a déjà été obtenu dans le cadre de la procédure de labellisation, doit tout d'abord, également être adapté dans la mesure où il est contraire à l'article 36, 4., du RGPD. L'article 24, paragraphe 1er, alinéa 2, doit quant à lui ensuite être supprimé, dès lors qu'il est redondant avec l'article 7, paragraphe 3, du projet.

75. **Plaintes.** Au sujet des plaintes, l'article 24/3, alinéa 2, du projet prévoit que la CCED est compétente pour recevoir les plaintes « à l'égard d'une autorité publique qui *aurait improprement exécuté une de ses obligations découlant du présent accord de coopération*, sans préjudice de l'application du RGPD » (italiques ajoutés par l'Autorité). Pour les raisons déjà évoquées (voir *supra*, point n° 73), le projet est sur ce point indûment restrictif : la CCED doit pouvoir recevoir et traiter toute réclamation relative à un traitement de données relevant de sa sphère de compétences.

76. **Droit d'accès indirect**. L'article 27 du projet prévoit un droit d'accès indirect à charge de la CCED. L'Autorité comprend que l'objectif de cette disposition est l'organisation d'un accès indirect par l'intermédiaire de la CCED, lorsque ce droit ne peut être exercé à l'égard d'une autorité publique relevant de sa compétence, ou lorsque plus généralement, il est dérogé par cette autorité, aux articles 12 à 22 du RGPD, en raison d'une disposition (une « loi », précise le projet) exécutant l'article 23 du RGPD. La formulation du paragraphe 1er, de l'article 27 devrait tout d'abord être clarifiée en ce sens.

77. Cela étant ensuite, l'Autorité réitère qu'elle est défavorable à la mise en place d'un système d'accès indirect et renvoie à ce sujet, à la position qu'elle a déjà exprimée[27]. Elle y est d'autant plus défavorable que l'article 27 du projet exige de la CCED qu'elle examine systématiquement s'il a été décidé correctement ou pas, de faire exception aux droits de la personne concernée.

78. Enfin, l'Autorité ne perçoit pas sur la base de quel fondement la CCED pourrait « saisir également le ministère public ou le juge d'instruction afin d'effectuer les vérifications nécessaires ». Cela est contraire à l'article 55, 3., du RGPD prévoyant que les autorités de contrôle ne sont pas compétentes pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelle.

Missions et pouvoirs : motivation, confidentialité et procédures

79. A propos des règles régissant l'exercice de ses missions et pouvoirs par la CCED, le projet consacre certaines règles qui seront d'abord évoquées dans la suite des développements, et prévoit

[27] Voir Avis de l'APD n° 06/2019 du 16 janvier 2019, point n° 11.

également des délégations aux Gouvernements et au règlement d'ordre intérieur de la CCED qui seront abordées ensuite. L'Autorité est d'avis que le projet doit être adapté en la matière.

80. **Modulation des mesures correctrices.** Concernant la modulation des mesures correctrices visées à l'article 58 du RGPD (celles-ci sont plus précisément consacrées dans l'article 58, 2., du RGPD), l'article 24/2, paragraphe 1er, du projet est ambigu lorsqu'il prévoit que lorsqu' « elle envisage une mesure correctrice, la [CCED] tient compte de la politique de sécurité de l'information et de l'état de la technique, des coûts de mise en œuvre, de la nature, de l'étendue, du contexte et des finalités du traitement, et des risques pour les droits et libertés des personnes ». Les mesures envisagées par une autorité de contrôle doivent l'être conformément au RGPD qui impose déjà la prise en compte de ces paramètres lorsqu'ils s'avèrent pertinents (voir par exemple, l'article 32, 1., du RGPD). Toute mesure correctrice ne doit pas, pour être prononcée, être analysée au regard de ces facteurs qui seront pris en compte, le cas échéant, dans l'analyse et la constatation de la violation du RGPD qui donnera lieu à la mesure correctrice concernée elle-même (par exemple, un avertissement, un rappel à l'ordre, etc.). La disposition en cause doit être adaptée en conséquence, et ce commentaire vaut *mutatis mutandis*, pour l'article 25, paragraphe 2, du projet (prévoyant l'obligation de motivation des avis, recommandations et autorisations de la CCED, et dans ce cadre, l'obligation de tenir compte des éléments précités).

81. **Motivation.** L'article 25, paragraphe 2, du projet prévoit que les avis, recommandations et autorisations de la CCED doivent être écrits et motivés. L'Autorité part du principe que pour les décisions prises par la CCED, la motivation sera requise en application de la loi du 29 juillet 1991 relative à la motivation formelle des actes administratifs.

82. **Droits de la défense.** Concernant les droits de la défense, l'article 24/2, paragraphe 1er, alinéas 2 et 4 prévoit, « le cas échéant », d'inviter l'autorité publique concernée à exercer « son droit à la défense » par écrit, dans un délai de dix jours. L'alinéa 4 précise que l'invitation préalable à exercer « les droits de la défense » n'est pas requise lorsque cela rendrait la mesure envisagée inefficace ou lorsqu'un retard supplémentaire porterait gravement atteinte à la protection des données. L'article 24/3, alinéa 2, du projet, prévoit encore que la CCED doit prévoir l'exercice « d'un droit de défense » dans le cas des procédures de réclamation. L'Autorité s'interroge sur la licéité d'une telle disposition au regard du respect des droits de la défense (voir notamment les articles 95, paragraphe 2, et 98 de la LTD), question ne relevant cependant pas de sa compétence.

83. **Confidentialité.** Quant à la confidentialité qui tient les membres et le personnel de la CCED, l'article 22/2, paragraphe 6, devrait prévoir plus généralement qu'ils ne sont pas tenus à la confidentialité dès lors que cela est nécessaire à l'exercice des missions de la CCED (voir également la source d'inspiration que peut constituer l'article 48, paragraphe 2, de la LCA).

84. **Délégations aux Gouvernements et ROI**. Sous l'angle des délégations, une marge de manœuvre significative est laissée au règlement d'ordre intérieur [ROI] de la CCED. Ainsi, l'article 22/3, paragraphe 1er, alinéa 3, prévoit que le ROI (*in fine*, soumis à l'approbation des Parlements) « contient en tout état de cause des règles relatives à la gestion financière à l'organisation administrative ainsi qu'aux méthodes et procédures de travail en vue de l'exercice correct et prudent des différentes tâches et compétences visées aux articles 57 et 58 du RGDP ». L'article 24/3, alinéa 2, du projet prévoit que la CCED organise la procédure de réclamation conformément à l'article 57, 1., f), et 2., du RGPD dans son ROI qui « prévoit l'exercice d'un droit de la défense ». Par ailleurs, les « Gouvernements des parties peuvent conjointement et, après avis de la [CCED], préciser les conditions particulières d'application des pouvoirs visés à l'article 58 du RGPD ».

85. **Lacunes du projet.** Bien que cela ne relève pas de sa compétence, l'Autorité s'interroge, au regard des développements précédents, sur la nécessité de compléter le projet quant aux pouvoirs de la CCED et aux procédures relatives à l'exercice de ceux-ci. A cet égard, l'Autorité :

- renvoie de manière générale le demandeur à la **LCA** en ce qu'elle définit les pouvoirs du service d'inspection (inspecteur général et inspecteurs), organise un recours à leur encontre, et définit les pouvoirs de la chambre contentieuse et la procédure devant celle-ci, ainsi que la voie de recours disponible devant la Cour des marchés ;

- recommande que le demandeur prévoie dans le projet le pouvoir de la CCED de **classer sans suite** (comparer avec les articles 91, paragraphe 2, 95, paragraphe 1er, et 100, paragraphe 1er, de la LCA), sauf à risquer de paralyser le fonctionnement de celle-ci ;

- rappelle l'obligation de mise en place d'un **recours juridictionnel effectif** à l'encontre des pouvoirs de la CCED. L'article 53, 4., du RGPD prévoit en effet que « L'exercice des pouvoirs conférés à l'autorité de contrôle en application du présent article est subordonné à des garanties appropriées, y compris le droit à un recours juridictionnel effectif et à une procédure régulière, prévues par le droit de l'Union et le droit des Etats membres conformément à la Charte ». L'Autorité attire en particulier l'attention du demandeur à ce sujet, sur l'article 47 de la Charte, l'article 6 de la CEDH et le Protocole n° 7 à la CEDH[28]. En l'état du texte de l'accord de coopération, l'Autorité part du principe que les voies de recours de droit commun seront ouvertes au responsable de traitement, et invite le demandeur à clarifier le jeu de celles-ci, en la matière, dans l'exposé des motifs du projet ;

[28] Voir encore Avis de la Commission de la Protection de la Vie Privée n° 29/2012 du 12 septembre 2012, points nos 53-54.

- enfin quant au respect des garanties consacrée dans l'article 6 de la CEDH (volet pénal), l'Autorité rappelle l'importance de **distinguer clairement les fonctions de poursuite, d'instruction et de sanction** de la CCED[29], sauf à se risquer à la violation de cet article.

Mécanisme de cohérence et coopération au niveau européen

86. L'Autorité rappelle qu'à cet égard, un accord de coopération sera nécessaire entre les différents pouvoirs (voir *supra*, point n° 30). Sont concernés par ce sujet, l'article 24, paragraphe 3, prévoyant la possibilité de réaliser des listes de traitements nécessitant ou pas une analyse d'impact relative à la protection des données ; l'article 24/2, paragraphe 3, qui prévoit que la CCED coopère avec d'autres autorités de contrôle et la Commission européenne conformément au chapitre VII du RGPD.

II.3. Responsabilités au regard des traitements

II.3.1. Principes

87. L'objectif de la définition large du concept de responsable du traitement[30] est d'assurer une protection efficace et complète des personnes concernées[31]. Selon les faits, une responsabilité conjointe de traitement peut lier plusieurs acteurs, la personne concernée [pouvant alors] exercer ses droits à l'égard de et contre chacun d'entre eux[32].

88. Toutefois, « l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente [… et a]u contraire, [l]es opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes du cas d'espèce »[33]. C'est dans « le cadre de ses responsabilités, de ses compétences et de ses possibilités » que le coresponsable veillera à la conformité de son activité aux règles de protection des données[34].

---

[29] Voir notamment à ce propos, Cour EDH, arrêt du 11 juin 2009 (DUBUS S.A. c/ FRANCE), req. n° 5242/04. Lire le document préparé par la Division de la recherche et de la bibliothèque, au sein de la Direction du jurisconsulte de la Cour européenne des droits de l'homme, « Guide sur l'article 6 de la Convention européenne des droits de l'homme, Droit à un procès équitable (volet pénal) », 2014, pp. 17-21.

[30] Les définitions de responsable du traitement et de sous-traitant sont définies à l'article 4, 7) et 8) du RGPD. Sur ces concepts, lire G29, Avis n° 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant" (WP169), 16 février 2010.

[31] CJUE (Gr. Ch.), 13 mai 2014 (GOOGLE SPAIN SL, GOOGLE INC. c/ AEPD), aff. C-132/12, point 34 ; CJUE (Gr. Ch.), 5 juin 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH), aff. C-210/16, point 28.

[32] Article 26, 3., du RGPD.

[33] CJUE (Gr. Ch.), 5 juin 2018 (UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIM c/ WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN GMBH), aff. C-210/16, point 43. Lire également, notamment, G29, Avis n° 1/2010 sur les notions de "responsable du traitement" et de "sous-traitant", 16 février 2010., p. 20.

[34] CJUE (Gr. Ch.), 13 mai 2014 (GOOGLE SPAIN SL, GOOGLE INC. c/ AEPD), aff. C-132/12, point 38.

89. Lorsque les finalités et les moyens de traitement sont déterminés par le droit national, « le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit [national] »[35]. Si les Etats membres peuvent préciser l'application des règles du GDPR dans des domaines particuliers où ils légifèrent afin de garantir en ces domaines, la cohérence et la clarté du cadre normatif applicable au traitement de données, ils ne peuvent à ce titre, déroger au RGPD ou se départir des définitions qu'il consacre[36]. Juger du contraire non seulement contrarierait la lettre du texte du RGPD, mais pourrait également mettre en péril l'objectif qu'il poursuit d'assurer un niveau cohérent et élevé de protection des personnes physiques.

II.3.2. Acteurs concernés par le projet et missions assumées

90. **Gestionnaire de source authentique ou de banque de données issues de sources authentiques.** Ce gestionnaire (article 1er, 1°*bis*, du projet) est l'autorité publique désignée par le décret ou l'arrêté de gouvernement instituant la source authentique qui est « responsable de manière exclusive de la collecte, du stockage, de la mise à jour, de l'enregistrement et de la destructions des données composant la source authentique ». Il « coordonne et gère » ces activités, « assure à tout moment, entre autres, la qualité des données ainsi que leur sécurité, tant au niveau technique qu'organisationnel » et « tient un historique des données, pour autant que cela soit nécessaire eu égard aux finalités avancées ». Nb : le deuxième tiret du paragraphe 1er de l'article 10 qui se borne à rappeler l'applicabilité du RGPD doit être supprimé.

91. **BCED** et **eWBS**. La BCED est un acteur central du système de partage de données. Elle est instituée au sein d'eWBS (article 11, paragraphe 1er, alinéa 1er, du projet), à savoir le service commun entre la Région wallonne et la Communauté française chargé de la simplification administrative et de l'administration électronique visé dans l'accord de coopération du 21 février 2013 entre la Région wallonne et la Communauté française organisant un service commun en matière de simplification administrative et d'administration électronique dénommé e-Wallonie-Bruxelles Simplification (article 2, 4°, du projet). La BCED bénéficie de « l'autonomie et de l'indépendance nécessaire pour remplir ses tâches » (article 11, paragraphe 1er, alinéa 1er, du projet).

92. L'article 11 du projet donne de nombreuses missions à la BCED parmi lesquelles : développer les normes, les standards et l'architecture de base nécessaire pour une mise en œuvre efficace de la technologie de l'information et de la communication à l'appui de la stratégie commune en matière de partage de données ; développer les projets et services englobant potentiellement l'ensemble des

[35] Article 4, 7), du RGPD. Concernant la détermination des obligations respectives des responsables conjoints du traitement, lire également l'article 26, 1., du RGPD.

[36] Lire article 6, 3., alinéa 2, et considérants nos 8 et 10 du RGPD.

autorités publiques et qui soutiennent cette stratégie ; gérer la collaboration avec les autres autorités en matière de partage de données et dans ce cadre, notamment, mettre en place les moyens techniques pour communiquer les informations entre elle et les sources authentiques, entre elle et les banques de données issues de sources authentiques, entre elle et les autorités publiques et entre elle et les destinataires ; toujours dans ce cadre, établir des accords clairs, sur la base d'une répartition des tâches, entre les parties concernées concernant qui effectue quels authentifications, vérifications et contrôles, à l'aide de quels moyens, et qui en assume la responsabilité, la manière dont les résultats des authentifications, vérifications et contrôles exécutés font l'objet d'un échange et d'une conservation électroniques sécurisés entre les parties concernées, la prise et la gestion des traces, et la manière dont il faut veiller à ce qu'une reconstruction complète puisse avoir lieu concernant quelle personne physique a utilisé un service ou une transaction déterminées concernant un citoyen ou une entreprise déterminés et quand, par le biens de quel canal et à quelles fins.

93. En outre, la BCED mettra à disposition des données provenant de sources authentiques ou de banques de données issues de sources authentiques (articles 6, paragraphe 1er, et 8, paragraphe 1er, du projet). Ainsi, les autorités publiques « utilisent la [BCED] pour accéder aux sources authentiques de données et aux banques de données issues de sources authentiques ainsi qu'aux sources authentiques externes de données sauf si cet accès n'est pas possible techniquement, et sauf exceptions fixées par ou en vertu d'une loi ou d'un décret » (article 12, paragraphe 2, du projet) (soulignement ajouté par l'Autorité). Et les gestionnaires de sources authentiques ou de banques de données issues de sources authentiques doivent autoriser la BCED à « consulter, copier et transmettre les données contenues dans lesdites sources ou banques » (article 12, paragraphe 1er, du projet). Nb : l'article 12, paragraphe 3, du projet doit être supprimé en ce qu'il se borne à répéter l'obligation consacrée à l'article 37 du RGPD, et l'Autorité souligne que l'alinéa 2 du paragraphe 4 de ce même article impose au délégué à la protection des données une tâche qui n'est pas celle d'un tel délégué au sens du RGPD (ce qui en soi, n'est pas interdit, voir article 38, 6., du RGPD).

94. La BCED a une mission d'intégrateur de services dans le cadre de laquelle elle peut « effectuer, en concertation avec les sources authentiques externes de données, un stockage des données qu'elle traite sous forme de copie, dans le but de rendre plus efficace la transmission ultérieure de l'information » et ce, dans le respect de certaines conditions (article 13 du projet) (soulignement ajouté par l'Autorité). En tout état de cause, cette activité ne pourra avoir lieu, pour ce qui concerne les sources authentiques externes de données, que dans la mesure où les règles régissant ces sources le permettent (voir l'article 2, 5°, du projet). Nb : l'Autorité profite de cette occasion pour souligner que tel que défini par le projet, le caractère « authentique » de la source externe de données n'a aucune portée : le texte doit être adapté afin de donner sens à ce concept[37].

[37] L'article 2, 5°, définit la source authentique externe de données comme une « base de données gérée par une autorité appartenant au niveau international ou fédéral, une autre Communauté ou Région, et les institutions ou personnes morales qui

95. L'article 2, 3°, b), du projet, définit l'intégrateur de service comme une institution légalement reconnue dont le « rôle principal est d'organiser et de faciliter l'échange de données issues de sources authentiques ou de banques de données issues de source authentiques entre les différentes autorités publiques et autorités fédérales, ainsi que d'offrir des services d'accès hautement sécurisés aux sources authentiques, dans le respect de la réglementation relative à la protection des données à caractère personnel » (soulignement ajouté par l'Autorité).

96. De manière générale, la BCED « assure à tout moment la sécurité des données et de leur transmission » (article 16 du projet) (soulignement ajouté par l'Autorité).

97. Quant à l'offre de services de la BCED, premièrement, la BCED doit, lorsque la CCED ne donne une autorisation de transmission que pour des données pseudonymisées ou rendues anonymes, assurer la pseudonymisation ou l'anonymisation des données. Nb : l'Autorité rappelle à cette occasion que seules les données anonymisées ne sont plus des données à caractère personnel[38], et le processus d'anonymisation[39] de données à caractère personnel constitue un traitement de données à caractère particulièrement sensible dès lors que son produit, les données anonymes, sort intégralement du champ d'application du RGPD. Le projet relève dans ce cas que la BCED peut jouer le rôle de tiers de confiance, ce concept étant défini à l'article 2, 3°, a), du projet.

98. Deuxièmement plus largement en tant que tiers de confiance, la BCED « offre des services qui accroissent la fiabilité de l'échange électronique de données et de l'enregistrement de données » (article 2, 3°, a), du projet) (soulignement ajouté par l'Autorité).

99. Et troisièmement, la BCED « peut fournir aux autorités publiques des services supplémentaires, comme l'agrégation de données provenant de différentes sources authentiques » (article 15, alinéa 1er, du projet), et elle peut encore « héberger des données issues de sources authentiques pour le compte des sources authentiques qui ne disposeraient pas des capacités matérielles ou techniques pour héberger et exposer leurs données » (article 15, alinéa 2, du projet).

100. Enfin la BCED peut « développer des moyens techniques pour diffuser et mettre à disposition du public des informations, y compris des données à caractère personnel lorsque celles-ci ont déjà été

en relèvent, ainsi que les personnes morales de droit privé qui sont chargées de tâches ou missions d'intérêt général ». Aucun critère ne permet dans cette définition, de distinguer une source « authentique » d'une autre qui ne le serait pas. Il s'est dégagé, lors d'un échange avec les demandeurs au sein de l'Autorité, qu'il en était ainsi dès lors qu'en effet, les droits applicables à ces sources externes de données utilisent leurs propres concepts et critères. Cela étant, dans l'hypothèse où la source externe de données n'est pas unique, une solution pourrait être de limiter le recours à la source externe dont la qualité se rapproche le plus des critères de labellisation et de l'objectif poursuivi par la source.

[38] Voir le considérant n° 26 et l'article 4, 1), du RGPD.

[39] Sur l'anonymisation, lire G29, Avis n° 5/2014 sur les Techniques d'anonymisation (WP216), 10 avril 2014.

rendues publiques ou ont vocation à être diffusées largement pour des raisons d'intérêt général » (article 18 du projet) (soulignement ajouté par l'Autorité). Il est à noter qu'il n'est en l'espèce plus question de données issues de sources authentiques ou de banques de données issues de sources authentiques, mais bien de toute donnée.

101. **DTIC et ETNIC**. Pour son fonctionnement, en vertu de l'article 19 du projet, la BCED est organisée en deux pôles. Il s'agit d'une part, d'un **pôle organisationnel** institué au sein d'eWBS (chargé des tâches afférant aux domaines de la gestion de projets, de l'accompagnement juridique et des services transversaux) et d'autre part, d'un **pôle informatique** chargé des missions techniques, principalement de développement et d'exploitation. Et ce pôle informatique « s'appuie », pour la Région wallonne « sur les services du Gouvernement wallon en charge de l'informatique administrative (**DTIC**) et, pour la Communauté française, sur l'Entreprise publique des Technologies nouvelles de l'Information et de la communication (**ETNIC**) » (gras ajouté par l'Autorité). Les deux pôles sont coordonnés au sein d'une interface centralisée (dont le projet ne détaille pas le fonctionnement).

102. **Comité de coordination de la Sécurité eWBS**. Ce comité (composé de conseillers en sécurité de l'information, voir l'article 20/1 du projet) est mis en place pour « gérer la sécurité des informations relatives aux activités » de la BCED (article 20 du projet). Il veille à la coordination et la convergence des politiques de la sécurité de l'information entre eWBS et son pôle informatique, il coordonne les activités en matière de sécurité de l'information du service eWBS, du DTIC et de ETNIC lorsque ces activités touchent à l'activité d'eWBS ou les services qu'eWBS met à disposition des administrations, et il émet des avis et recommandations sur les projets d'eWBS liés au partage de données et à la simplification administrative.

103. **Autorités publiques destinataires des données**. Enfin bien entendu, il ne faut pas perdre de vue dans ce contexte, les autorités publiques qui accèderont aux sources authentiques et banques de données issues de sources authentiques de données afin de réaliser leurs missions d'intérêt public.

II.3.3. Allocation des responsabilités au regard du traitement de données à caractère personnel

104. Dans le contexte juste exposé, le projet ne prévoit pas explicitement d'allocation de responsabilités *au regard du traitement des données à caractère personnel en tant que tel*, mais bien plus généralement au regard du traitement des données des sources authentiques et banques de données issues de sources authentique. Or dans le cadre du présent projet, la détermination des responsabilités au regard du traitement des données à caractère personnel constitue indiscutablement un élément essentiel du traitement qui, conformément aux principes rappelés précédemment (voir *supra* points nos 5-6 et 87-89) et pour des raisons évidentes de sécurité juridique, doit être tranché

dans le dispositif du projet. Dans les développements suivants, l'Autorité illustre la tâche à encore accomplir dans le dispositif du projet.

105. **Utilisation de données provenant d'une source authentique par une autorité publique**. Il s'agit d'une hypothèse de base de partage de données entre autorités publiques. Le gestionnaire « A » gère une source authentique au sein de laquelle se situe une donnée dont le traitement est nécessaire à l'autorité publique « B », en vue de l'accomplissement de sa mission d'intérêt public ou relevant de l'exercice de l'autorité publique, par exemple l'octroi d'un permis à la personne concernée. Autorisée par la CCED, « B » accède à la donnée auprès de « A » via la BCED conformément à l'accord de coopération et au décret qui créée la source authentique, et traite ensuite les données conformément aux règles régissant l'octroi du permis concerné. Le système de partage de données mis en place par l'accord de coopération n'est que le support/le moyen à la collecte de la donnée nécessaire à l'autorité « B », et l'ensemble des opérations de traitement en cause ne constitue qu'un seul et même traitement répondant à la finalité de délivrance du permis à la personne concernée.

106. Au regard des tâches du gestionnaire de la source authentique (voir *supra*, point n° 90), des missions de la BCED (en particulier, celles d'intégrateur de services, voir *supra*, point nos 91-96 et 98) et de la mission de l'autorité publique qui accède à la donnée concernée (qui sera définie dans la norme consacrant ses missions), l'Autorité est d'avis que ces trois acteurs à tout le moins, sont responsables conjoints du traitement. Le projet demeurant libre pour le surplus, dans les limites permises par le RGPD, d'allouer entre eux les responsabilités individuelles de chacun, par exemple de la manière dont il alloue en l'état, les responsabilités au regard des différentes opérations de traitement en général (c'est-à-dire, indépendamment de la nature à caractère personnel ou non des données concernées) (collecte, stockage, mise à jour, sécurité, mise à disposition, etc.).

107. Ce constat appelle quatre commentaires. Premièrement, s'agissant d'une responsabilité conjointe au regard du traitement, l'Autorité rappelle que la personne concernée aura le droit, en vertu de l'article 26, 3., du RGPD d'exercer ses droits à l'égard de et contre chacun des responsables du traitement. Elle ne pourra donc être contrainte à subdiviser sa demande selon l'aspect concerné, auprès de l'un et l'autre intervenant.

108. Deuxièmement, en l'état du projet, l'Autorité ne perçoit pas précisément la manière dont fonctionneront les relations entre BCED, ETNIC, DTIC, eWBS et la manière dont les décisions seront prises dans ce contexte, au regard du traitement de données à caractère personnel. eWBS jouit d'une certaine indépendance tout en étant toutefois établie au sein d'eWBS qui est un service commun des gouvernements wallon et de la communauté française. DTIC est un service du gouvernement wallon

et ETNIC est une « entité autonome », un « organisme d'intérêt public »[40] dépendant de la Communauté française (voir *supra*, points nos 101 et 102). L'Autorité est d'avis que les relations entre ces entités et leurs responsabilités doivent être clarifiées, étant entendu qu'en l'état, ces entités semblent solidairement responsable au regard de la responsabilité encourue par la BCED (eWBS) elle-même, et en conséquence, responsables conjoints du traitement au même titre que cette dernière.

109. Dans la même logique, l'Autorité ne peut non plus *a priori* exclure que le comité de coordination de la Sécurité eWBS n'encoure une certaine responsabilité dès lors qu'il semble avoir une existence propre et poursuivre une mission déterminante au regard des questions de sécurité (voir article 20 à 20/3 du projet, et *supra*, point n° 102).

110. Troisièmement, il semble que des termes du projet (voir l'article 2, 1°*bis* et 2°*bis*) les gestionnaires de sources authentiques et de banque de données issues de sources authentiques ne sont pas responsables de la mise à disposition des données qu'ils traitent (ils seraient seulement responsables des collecte, stockage, mise à jour et destruction des données). Cette responsabilité incomberait plutôt à la BCED (voir notamment les articles 6, paragraphe 1er, et 8, paragraphe 1er du projet). L'Autorité s'interroge donc, du point de vue de la protection des données, si le demandeur envisage d'imputer la responsabilité dans la mise à disposition des données en cause exclusivement à la BCED. L'Autorité doute de la validité d'une telle approche, qui aurait pour effet d'ôter au gestionnaire de la source authentique de données la maîtrise de sa base de données. L'Autorité est d'avis que dans la responsabilité conjointe qu'il encourt, le gestionnaire de la source authentique de données encourt une responsabilité dans la mise à disposition des données issues de la source qu'il gère[41].

111. Quatrièmement enfin, l'Autorité souligne que les accords que la BCED pourra établir « sur la base d'une répartition des tâches, entre les parties concernées » concernant une série de points (dont la journalisation des accès, les authentifications à effectuer, etc.) ne peuvent déroger aux allocations de responsabilités directement réalisées par l'accord de coopération ou les autres règles qui régiront le traitement des données issues de sources authentiques ou de banques de données issues de sources authentiques (à savoir les textes qui établisses ces sources et banques de données, ainsi que les textes qui régissent les activités de traitement de données par les autorités publiques qui y accèderont via la BCED).

112. **Autres responsabilités probables de la BCED**. Il convient encore de déterminer dans le projet, le responsable du traitement des traitements de données d'anonymisation et de

[40] Voir http://www.etnic.be/letnic/histoire/.

[41] Dans le même sens, la Commission de la Protection de la Vie Privée avait rappelé « que la source authentique doit – éventuellement avec l'intervention de la banque-carrefour d'échange de données – garantir le respect du principe de proportionnalité. Il est en effet uniquement permis de collecter/conserver/transmettre des données pertinentes et non excessives », Avis de la Commission de la Protection de la Vie Privée n° 29/2012 du 12 septembre 2012, point n° 54.

pseudonymisation (voir *supra*, point n° 97), des traitements d'agrégation de données provenant de sources authentiques (voir *supra*, point n° 98) et encore, des traitements de mise à disposition du public de données (voir *supra*, point n° 100) (voir *supra*, point n° 24). *A priori*, la BCED semblerait être responsable de ces traitements, le cas échéant conjointement avec les autorités qui aurait recours à ces services. L'Autorité ne peut analyser ces traitements, leurs finalités n'étant pas déterminées dans le projet.

113. Ce dernier semble enfin laisser entendre que la BCED pourrait avoir un rôle de sous-traitant lorsqu'elle héberge des données, ce qui devrait également être clarifié (voir *supra*, point n° 97).

II.3.3. Mesures techniques et organisationnelles – sécurité – et obligation de recourir à la BCED

114. Eu égard au rôle central joué par la BCED qui comme son nom l'indique, constitue un véritable carrefour de l'échange de données, l'Autorité est d'avis que le dispositif ne peut être muet quant à son obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées au regard des risques auxquels sont exposés les droits et libertés des personnes concernées (article 32 du RGPD).

115. A cet égard, l'Autorité est favorable aux dispositions prévues dans le projet en la matière (voir les articles 10, 11, paragraphe 2, 8), g), 12, paragraphe 4, 13, 16 et 20), et en particulier au fait qu'en tant qu'intégrateur de services, la BCED doit offrir des services d'accès « hautement sécurisés » aux sources authentiques dans le respect de la réglementation applicable (article 2, 3°, b) du projet).

116. L'Autorité considère néanmoins que cette exigence d'un niveau élevé de sécurité devrait plus généralement être consacrée dans l'article 16 du projet, première phrase, qui prévoit que la BCED « assure à tout moment la sécurité des données et de leur transmission ». Plus généralement, le dispositif devrait prévoir que la BCED doit assurer un niveau de sécurité élevé des traitements relevant de l'exercice de ses missions. Au-delà de ce point spécifique, des règles et concepts consacrés dans la législation applicable dans d'autres domaines[42] pourraient le cas échéant être sollicités, en vue de renforcer le dispositif sous l'angle des mesures techniques et organisationnelles à mettre en place par la BCED.

[42] Voir le Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. Notamment, son article 8 prévoit trois niveaux de garantie des schémas d'identification électronique (faible, substantiel ou élevé). Pour ce qui concerne les services de confiance, c.-à-d. notamment la signature électronique, les exigences de sécurité varient selon qu'il est question de service qualifiés ou non qualifiés. Concernant la signature électronique qualifiée, lire par exemple les articles 28 et 29 du règlement. Voir également, en ce qui concerne l'archivage électronique, le Titre 2 du Livre XII du Code de droit économique. Dans un autre domaine, celui des opérateurs de services essentiels, voir La Directive (UE) n° 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

117. Enfin, l'Autorité émet des réserves quant à l'obligation consacrée dans l'article 6 du projet, selon laquelle les autorités publiques de la Région wallonne et de la Communauté française sont obligées de faire appel à la BCED pour l'échange électronique de données (sans préjudice des critiques déjà émises à l'encontre du recours aux banques de données issues de sources authentique, voir *supra*, points nos 13-16). Nonobstant les bonnes intentions d'une telle disposition, elle peut avoir un effet non souhaité, notamment qu'une autorité ne reçoive pas des données provenant d'une instance fédérale ou flamande. Un responsable du traitement qui fournit des données va préalablement à la fourniture de celles-ci, forcément, souhaiter avec certitude que l'intégrateur de services concerné offre son service conformément aux obligations consacrées dans le RGPD. Si tel n'est pas le cas, le responsable du traitement va refuser de fournir les données et l'autorité qui demande les données s'en retrouvera mise en difficulté. Vu son obligation en vertu du projet, cette dernière ne pourra pas faire appel à un autre intégrateur de service qui offre bel et bien de telles garanties.

118. Pour un intégrateur de services, travailler conformément au RGPD signifie de participer à un accord de coopération qui est décrit comme « cercles de confiance »[43], et l'article 11, paragraphe 2, 8), g), du projet peut être amélioré à cet égard. Ceux-ci sont réalisés au moyen d'une répartition des tâches entre les instances concernées qui concluent des accords clairs sur :

- qui réalise le contrôle de la proportionnalité des données échangées (filtrage, répertoire des références) ;

- qui effectue quelles authentifications, quelles vérifications et quels contrôles à l'aide de quels moyens et qui en est responsable ;

- la manière dont les résultats des authentifications, vérifications et contrôles effectués sont échangés de manière sûre par voie électronique entre les instances concernées ;

- quel chiffrement est exigé ;

- qui maintient quels loggings ;

- la manière dont on veille à ce que puisse avoir lieu, lors d'un examen effectué à l'initiative d'un organe de contrôle ou à l'occasion d'une plainte, un traçage complet de la personne physique qui a utilisé quel service ou quelle transaction concernant quel citoyen ou quelle entreprise, quand, via quel canal et pour quelles finalités.

[43] Voir à ce propos la Recommandation de la Commission de la Protection de la Vie Privée n° 03/2009, points nos 13 à 15.

III. CONCLUSION

PAR CES MOTIFS,

l'Autorité est d'avis que le projet d'accord de coopération modifiant l'accord de coopération du 23 mai 2013 entre la Région wallonne et la Communauté française portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative **doit être adapté**. Les adaptations à réaliser peuvent être synthétisées comme suit.

Avant de récapituler en synthèse les différentes adaptations à apporter au projet, l'Autorité souhaite attirer l'attention des demandeurs sur les trois éléments suivants, revêtant une importance particulière :

- premièrement, les sources authentiques de données ne peuvent pas être dupliquées par un intégrateur de service ou une autre autorité publique, sauf à méconnaître leur principe et potentiellement, les règles qui les établissent et les réglementent, en particulier lorsque ces sources sont régies par un autre niveau de pouvoir ;

- deuxièmement l'intervention de plusieurs intégrateurs de services sans une bonne répartition de leurs tâches respectives et sans des engagements mutuels en matière de sécurité de l'information, est contraire aux obligations consacrées dans le RGPD en matière de sécurité de l'information ;

- troisièmement enfin, l'Autorité est défavorable au projet en ce qu'il octroie également à une autorité de contrôle, une compétence d'autorisation normative générale concernant l'ensemble des flux de données issues de sources authentiques entre autorités publiques, compétence qui devrait relever de la responsabilité des responsables du traitement et le cas échéant, d'une entité instituée à cet effet, au titre de l' « *accountability* ».

Concernant les concepts utilisés par le projet, la réutilisation des données généralisées mise en place et les principes de transparence et légalité :

- le concept de banque de données issues de sources authentiques devrait être abandonné dès lors qu'il n'est pas conforme à la logique même des sources authentiques, en particulier dans la mesure où il pourrait comprendre également des sources authentiques externes, organisées à un autre niveau de pouvoir. En tout état de cause, d'une part, il ne pourrait être

mis en œuvre que dans le respect des cadres normatifs régissant ces sources externes, et des clarifications doivent encore y être apportées (points nos 13-16) ;

- des critères doivent encadrer la labellisation (point n° 17) ;

- le projet devra garantir, dans le système de réutilisation généralisée des données issues de sources authentique et de banques de données issues de sources authentiques qu'il met en place, le respect des principes de transparence et de légalité consacrés dans les articles 8 et 22 de la Constitution, c'est-à-dire la précision des éléments essentiels des traitements dans des normes du rang de loi (décrets en l'occurrence) (point n° 19) ;

- et il le devra également plus spécifiquement, à l'égard des traitements de données qui découlent directement de son application, en l'occurrence les traitements qui seront réalisés par la CCED dans l'exercice de ses missions (points n° 24, 68 et s., et 115).

En ce qu'il crée une autorité de contrôle au sens du RGPD, la CCED :

- le projet doit tout d'abord déterminer clairement la compétence de cette autorité au regard des règles répartitrices de compétences et des questions qu'elles soulèvent (points nos 25-49) ;

- il doit également prévoir que la CCED exerce toutes ses missions et pouvoirs à l'égard de l'intégralité de cette sphère de compétence (points nos 51-54, 73 et 75). Ainsi, les missions de la CCED en matière de plaintes et avis doivent être étendues à l'ensemble des traitements réalisés par les autorités publiques et ne peuvent être limitées à l'application de l'accord de coopération ;

- bien que l'Autorité considère que la collaboration entre autorités de contrôle doive faire l'objet d'un accord de coopération entre l'ensemble des entités fédérale et fédérées, le projet doit néanmoins être amélioré sur ce point (points nos 55-58 et 86) : l'expression veiller à la compatibilité des avis et recommandations de la CCED avec les décisions de l'Autorité doit être clarifiée, la soumission à l'avis préalable de l'Autorité (si elle pouvait être organisée en dehors de la LCA) doit être accompagnée de l'analyse nécessaire et la licéité de la délégation des pouvoirs d'investigation pose question ; un accord de coopération sera nécessaire en ce domaine ;

- en outre, les règles qui régissent d'une manière ou d'une autre, l'indépendance de la CCED doivent être renforcées (points nos 59-64) : le concept d'indépendance ne doit pas être défini

comme il l'est par le projet, quant aux conditions applicables aux membres, les règles relatives aux incompatibilités et conflits d'intérêts doivent être améliorées à la lumière de la LCA, le représentant de la BCED ne devrait pas systématiquement participer aux réunions de la CCED et cette dernière doit être dotée des ressources humaines et budgétaires propres et nécessaires à l'exercice de ses nombreuses compétences.

Concernant les pouvoirs et missions de la CCED :

- le choix ou non de donner à la CCED le pouvoir de prononcer des amendes administratives, qui semble être posé pour peu que les règles répartitrices de compétences l'autorise, doit être clarifié (points nos 65-66) ;

- l'Autorité doute de la conformité de la large compétence d'autorisation de la CCED par rapport à l'approche fondée sur le risque préconisée par le RGPD et suivie par ailleurs à d'autres niveaux de pouvoir et souligne la possible redondance d'un tel mécanisme (points nos 68-71) ;

- l'Autorité doute aussi de l'efficacité de la mise en place d'un droit d'accès indirect, dont la formulation doit en tout état de cause, être adaptée (points nos 76-78) ;

- enfin, concernant les règles applicables à l'exercice par la CCED de ses pouvoirs, l'Autorité s'interroge sur la largesse de la délégation faite aux Gouvernements et au ROI, et est d'avis que le projet comporte une série de lacunes auxquelles il convient de remédier (point n° 85) : la LCA peut être une source d'inspiration concernant la définition des pouvoirs et procédures en cause, la CCED devrait avoir un pouvoir de classement sans suite, le projet doit clarifier le recours juridictionnel effectif ouvert au responsable de traitement à l'encontre des pouvoirs de la CCED et enfin, le projet doit distinguer clairement les fonctions de poursuite, d'instruction et de sanction de la CCED, conformément à l'article 6 CEDH.

L'Autorité est encore d'avis que le projet doit clarifier les responsabilités des différents acteurs impliqués par le projet (gestionnaires de source authentique et de banque de données issues de source authentique, autorité publique qui réutilise des données, eWBS, BCED, DTIC, ETNIC et Comité de coordination de la Sécurité eWBS) au regard des traitements de données à caractère personnel, le projet ne désignant en l'état et *stricto sensu*, aucun responsable du traitement (points nos 90-113).

En particulier concernant la BCED :

- le projet pourrait exiger plus généralement, que la BCED garantisse un haut niveau de sécurité dans le cadre de l'ensemble de ses activités (points nos 114-116) ;

- l'Autorité émet des réserves quant à l'obligation consacrée dans l'article 6 du projet, selon laquelle les autorités publiques de la Région wallonne et de la Communauté française sont obligées de faire appel à la BCED pour l'échange électronique de données, au regard des problèmes pratiques susceptibles de résulter d'une telle obligation (point 117) ;

- et elle rappelle enfin l'importance pour la BCED de travailler en « cercles de confiance » (point 118).

Enfin, plus ponctuellement :

- certaines dispositions du projet doivent être omises dans la mesure où elles répètent des règles du RGPD, voir : points n° 11, concernant les statistiques notamment ; point n° 67, concernant la compétence de contrôle de la CCED sur la BCED ; point n° 80, concernant la motivation des mesures correctrices ;

- et d'autres dispositions doivent être précisées ou adaptées, voir : point n° 20, concernant l'exception à l'obligation de collecte unique notamment ; points nos 22-23, à propos du moyen électronique à mettre en place en vue de permettre l'exercice partiel du droit d'accès au sujet duquel la personne concernée devrait être correctement informée ; point n° 83, concernant l'obligation de confidentialité applicable au personnel et membres de la CCED qui devrait être nuancée.

(sé) An Machtens
Administrateur f.f.

(sé) Willem Debeuckelaere
Président,
Directeur du Centre de connaissances