Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 154/2023 du 20 octobre 2023

Objet: Demande d'avis concernant un avant-projet de décret et ordonnance conjoints portant le code bruxellois de la gouvernance et de la donnée (CO-A-2023-407)

Version originale

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Juline Deschuyteneer et Cédrine Morlière et Messieurs Bart Preneel et Gert Vermeulen;

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 l'article 25, alinéa 3, de la LCA selon lequel les décisions du Centre de Connaissances sont adoptées à la majorité des voix ;

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 du Ministre du Gouvernement de la Région de Bruxelles-Capitale, chargé de l'Emploi et de la Formation professionnelle, de la Transition numérique, des Pouvoirs locaux et du Bien-être animal, Monsieur Bernard Clerfayt (ci-après « le Ministre »), reçue le 25 juillet 2023 ;

Émet, le 20 octobre 2023, l'avis suivant :

I. Objet et contexte de la demande d'avis

1. Le Ministre a introduit auprès de l'Autorité une demande d'avis concernant l'ensemble des dispositions d'un avant-projet de décret et ordonnance conjoints *portant le code bruxellois de la gouvernance et de la donnée* (ci-après, « le Projet »). Le demandeur précise dans le formulaire de demande d'avis que « *L'avant-projet de décret et ordonnance conjoints portant le code bruxellois de la gouvernance et de la donnée a pour objectif de codifier l'ensemble des législations et règlementations internes et européennes en matière de données et de gouvernance* ».

II. Examen

Le présent avis est structuré comme suit :

II.1. Considérations générales 3
II.1.1. Portée du Projet et précédents avis de l'Autorité 4
II.1.2. Préoccupation générale et importante causée par le Projet sur le plan de la protection des données 7
A) Facilitation du traitement des données, de leur circulation entre autorités et de leur concentration 8
B) Le CIRB (PARADIGM), une institution centrale et incontournable du traitement de données 10
C) Une certaine conception patrimoniale de la donnée aux conséquences concrètes floues 16
II.1.3. Commentaires généraux concernant le Projet 19
II.2. Transparence administrative 21
II.2.1. Publicité passive et intérêt 21
II.2.2. Communication des données par courriel 22
II.2.3. Rôle du consentement (informations environnementales) 24
II.2.4. Soustraction partielle à la publicité administrative 25
II.2.5. Publication de données via internet 25
II.4. Partage administratif de données (échanges de données entre autorités publiques) (Livre C.IV., Titre 2) 27
II.4.1. Partage administratif en général 28
II.4.2. Sources authentiques de données 30
II.4.3. Base de données issues de sources authentiques 35
II.5. Réutilisation des documents et des données publiques (Livre C.IV, Titre 3) 38
II.5.1. Portée des deux régimes de réutilisation 38
II.5.2. Transposition de la Directive Réutilisation – articles C.IV.17 à C.IV.30 40
II.5.3. Exécution du Règlement sur la Gouvernance des Données – articles C.IV.31 à C.IV.32 41
II.5.4. Publication de données à caractère personnel 49
II.5.5. Altruisme en matière de données 50

II.6. Commission d'accès aux documents administratifs et aux données (« CADADO »)50
II.6.1. Un organe de recours et d'avis différent d'une autorité de protection des données.....50
II.6.2. Communication systématique de données à la CADADO 51
II.6.3. Autres pouvoirs de la CADADO.....52
II.6.4. Avis de l'Autorité de Protection des Données 52
II.6.5. Publication des décisions de la CADADO 53
II.7. Gouvernance de la donnée 54
II.7.1. Champ d'application (indéterminé) et portée obligatoire des règles du Code.....54
II.7.2. Régimes juridiques applicables aux données 55
II.7.3. Réversibilité des données 55
II.7.4. Typologie des catégories de données 56
II.7.5. Valorisation des données d'usage.....57
II.7.6. Respect du droit des tiers dans la valorisation des données – consentement et al. 58
II.7.7. Recours dans le cadre de la valorisation des données.....61
II.7.8. Mise à jour des données.....62
II.7.9. Données de référence 63
II.7.10. Modèles analytiques, algorithmes et intelligence artificielle 64
II.8. ResponsabilitéS au regard du traitement de données à caractère personnel 65
II.9. Centre d'exploitation et d'analyse des données 68
II.10. Durée de conservation des données 68
II.11. Désignation d'URBIS comme banque de données issues de sources authentiques 72
II.12. Conclusion 74

II.1. CONSIDÉRATIONS GÉNÉRALES

2. L'Autorité relève d'emblée que l'approche suivie par le demandeur apparaît audacieuse et novatrice. Globalement, l'Autorité ne peut que se satisfaire des initiatives poursuivant pour objectif le renforcement de la qualité de la gestion et de la gouvernance des données même au-delà des données à caractère personnel, une telle approche étant de nature à renforcer l'attention du responsable du traitement à l'égard de la manipulation de la donnée en général et donc, de la donnée à caractère personnel également.

3. Ce mérite étant reconnu à l'objectif poursuivi par le Projet transversal soumis pour avis, l'Autorité souligne néanmoins que ce dernier soulève certaines préoccupations importantes et nécessite plusieurs commentaires sur le plan de la protection des données. Par souci d'efficacité, le présent avis est centré

sur ceux-ci et ne peut cataloguer par la même occasion, l'ensemble des éventuels aspects positifs du Projet.

II.1.1. Portée du Projet et précédents avis de l'Autorité

4. Le Projet régit de manière codifiée, la **transparence administrative** (ou publicité de l'administration, active et passive), la **réutilisation des informations** du secteur public, **l'échange de données entre autorités publiques** (y compris concernant les sources authentiques et les banques de données issues de sources authentiques) et les **principes applicables à la gouvernance** des données par ces autorités (le Projet mettant en place sur ce point, un nouveau paysage institutionnel). Il consacre en outre **une banque de données issues de sources authentiques bruxelloises majeures**, « *Brussels UrbIS* »[1].

5. A ces fins, sur le plan législatif, l'article 20 du Projet **abroge les textes suivants** :

   - L'ordonnance du 17 juillet 2020 *garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité, et portant simplification et harmonisation des formulaires électroniques et papier* ;

   - Les décret et ordonnance conjoints du 16 mai 2019 de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française *relatifs à la publicité de l'administration dans les institutions bruxelloises* ;

   - L'ordonnance du 27 octobre 2016 *visant à l'établissement d'une politique de données ouvertes (Open Data) et portant transposition de la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public* ;

   - L'ordonnance du 8 mai 2014 *portant création et organisation d'un intégrateur de services régional*.

6. En matière de **transparence administrative** et en particulier, de publication de données à caractère personnel, l'Autorité a récemment récapitulé sa position dans les deux avis suivants :

[1] Soit, selon l'article 3, 6°, du Titre III du Projet, la « *banque de données de fichiers vectoriels et images de cartographie numérique de référence à grande échelle du territoire de la Région de Bruxelles-Capitale faisant partie du produit UrbIS distribué par le CIRB conformément à l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 19 mai 1994 relatif à la mission de promotion, de distribution et de services aux utilisateurs du produit Brussels UrbIS* ».

- Avis n° 131/2023 du 8 septembre 2023 *concernant un amendement n° 4 du projet de loi modifiant la loi du 11 avril 1994 relative à la publicité de l'administration et abrogeant la loi du 12 novembre 1997 relative à la publicité de l'administration dans les provinces et les communes (CO-A-2022-316)* (ci-après, « **l'avis n° 131/2023** »);

- Avis n° 42/2023 du 9 février 2023 *concernant un avant-projet de loi modifiant la loi du 11 avril 1994 relative à la publicité de l'administration (CO-A-2022-311)* (ci-après, « **l'avis n° 42/2023** »).

7. En ce qui concerne la **réutilisation des informations du secteur public**, l'Autorité invite le demandeur à se référer à titre préliminaire aux avis suivants dont les principes sont applicables :

- Avis n° 144/2023 du 29 septembre 2023 *concernant un avant-projet de loi modifiant la loi du 4 mai 2016 relative à la réutilisation des informations du secteur public (CO-A-2023-334)* (ci-après, « **l'avis n° 144/2023** ») ;

- Avis n° 203/2021 du 25 octobre 2021 *concernant un projet de décret n° 2020/279 de la Commission communautaire française relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2021-196)* (ci-après, « **l'avis n° 203/2021** ») ;

- Avis n° 167/2022 du 19 juillet 2022 *concernant un avant-projet de décret relatif à la diffusion et à la réutilisation des informations du secteur public, et un avant-projet de décret relatif à la diffusion et à la réutilisation des informations du secteur public pour les matières réglées à l'article 138 de la Constitution (CO-A-2022-150)* (ci-après, « **l'avis n° 167/2022** »);

- Avis n° 227/2022 du 29 septembre 2022 *concernant un avant-projet de décret relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2022-209)*.

8. À propos de **l'échange de données issues de sources authentiques de données**, les intégrateurs de service et les responsabilités y liées au regard du traitement de données à caractère personnel, l'Autorité invite le demandeur à se reporter à son avis n° 143/2023 du 29 septembre 2023 *concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-375), et concernant un avant-projet de décret portant assentiment à l'accord de coopération entre la Région wallonne et la Communauté française désignant l'intégrateur de services de la Région wallonne et de la Communauté française et un projet*

d'accord de coopération relatif à la création du service commun aux Gouvernements Wallon et de la Communauté française, dénommé Banque Carrefour d'échange de données (non soumis à assentiment) (CO-A-2023-376) (ci-après, « **avis n° 143/2023** »)

9. Le Projet **s'inscrit en outre pour partie dans le droit européen**, sans qu'il soit nécessaire de lister tous les textes européens auxquels il fait référence, peuvent être cités la Directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 *modifiant la Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public* (ci-après, « **la Directive Réutilisation** »), et le Règlement 2022/868 du Parlement européen et du Conseil du 30 mai 2022 *portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données)* (ci-après, « **le Règlement sur la Gouvernance des Données** ») qu'il exécute partiellement, qui seront pris en compte ultérieurement dans le présent avis.

10. Dans ce contexte, **le Projet consacre plus de 120 définitions**, tantôt existantes, tantôt inspirés du droit européen, du droit fédéral ou encore, de la doctrine, lorsque le Projet consacre de nouveaux concepts. A titre illustratif, les concepts suivants sont définis par le Projet (les concepts mis en gras sont sollicités dans la suite de l'avis et définis en note de bas de page) : « *autorité publique* » ; « ***autorité publique tierce*** »[2] ; « *donnée* » ; « ***donnée protégée*** »[3] ; « *donnée sensible* » ; « ***donnée publique*** »[4] ; « *donnée classifiée* » ; « *jeu de données* » ; « ***donnée ouverte*** »[5] ; « *donnée acquise* » ; « *donnée déduite* » ; « *donnée dérivée* » ; « *donnée d'origine privée* » ; « *donnée exclusive* » ; « *donnée fermée* » ; « *donnée fournie librement* » ; « *donnée observée* » ; « ***donnée d'usage*** »[6] ; « *donnée de contenu* » ; « ***donnée de référence*** »[7] ; « *métadonnée* » ; « *donnée issue de source authentique* » ; « ***source authentique*** »[8] ; « ***utilisateur (des***

---

[2] Soit, selon l'article A.III.1.5), « *pouvoir public relevant d'un autre niveau de pouvoir, à savoir national ou international* ».

[3] Soit, selon l'article A.III.1.9) du Projet :

« *toute donnée qui est protégée pour l'un des motifs suivants :*

(a) confidentialité commerciale, y compris le secret d'affaires, le secret professionnel et le secret d'entreprise ;

(b) secret statistique ;

(c) protection des droits de propriété intellectuelle de tiers ;

(d) protection des données à caractère personnel ».

[4] Soit, selon l'article A.III.1.23) du Projet, « *toute donnée détenue et gérée par les Autorités publiques dans le cadre de leurs missions de services publics* ».

[5] Soit, selon l'article A.III.1.13) du Projet, « *toute donnée librement accessible* ».

[6] Soit, selon l'article A.III.1.24) du Projet, « *toute donnée issue de l'activité d'un utilisateur de données et, plus spécifiquement, de son interaction avec des données ; les données d'usage sont collectées afin de fournir de l'information sur l'utilisateur* ». L'utilisateur (des données) est défini par l'article A.III.1.34) comme l' « *utilisateur défini au sens de l'article 2, 9) du* [Règlement Gouvernance des Données] », soit « *une personne physique ou morale qui dispose d'un accès licite à certaines données à caractère personnel ou non personnel et qui a le droit, y compris au titre du règlement (UE) 2016/679 lorsqu'il s'agit de données à caractère personnel, d'utiliser ces données à des fins commerciales ou non commerciales* ».

[7] Soit, selon l'article A.III.1.26) du Projet, « *toute donnée considérée comme structurante, par l'Autorité publique ou par l'usage, notamment pour nommer ou identifier des produits, des entités économiques, des territoires ou des personnes physiques et morales* ».

[8] Voir le considérant n° 69.

données)»[9] ; « ***tiers de confiance*** »[10] ; « *administrateur de base de données* » ; « *service d'intermédiation de données* » ; « *écosystème numérique bruxellois* » ; « *plateforme bruxelloise de la donnée* » ; « *Centre d'intégration bruxellois* » ; « *Centre d'exploitation et d'analyse des données* » ; « *autorité publique producteur* » ; « ***valorisation*** »[11] ; « *partage de données* » ; « ***partage administratif*** »[12] ; « *communication* » ; « *occultation* » ; « ***intégration des données*** »[13] ; « ***interopérabilité*** »[14] ; « *intelligence artificielle* » ; « ***partenariat numérique*** »[15].

11. Compte-tenu de sa portée et de son domaine très vaste d'application, y compris les choix posés notamment dans le domaine de la réutilisation des données[16], il est clair que le Projet présente une **ingérence importante** dans les droits et libertés des personnes concernées.

II.1.2. Préoccupation générale et importante causée par le Projet sur le plan de la protection des données

12. Au-delà de sa large portée, sans préjudice des commentaires ultérieurs, l'Autorité est d'avis qu'en outre, **le Projet soulève une préoccupation générale et importante sur le plan de la protection des données et ce, pour les trois motifs suivants** :

- Le dispositif du Projet tend à **faciliter significativement le traitement des données par les autorités publiques bruxelloises et en particulier, la circulation des données entre ces autorités,** notamment en poursuivant une dynamique de concentration dans le domaine du traitement de données (intégration de services et de données, interopérabilité, mutualisation) ;

---

[9] Voir la note de bas de page n° 6.

[10] Soit, selon l'article A.III.1.98) du Projet, « *une entité indépendante qui dispose des moyens techniques nécessaires à l'anonymisation ou la pseudonymisation des données à caractère personnel dans le cadre des traitements énoncés par l'article 89 du RGPD* ».

[11] Soit, selon l'article A.III.1.68), « *traitement de données en vue de les exploiter de manière à optimiser les missions de services publics ou les obligations légales dont sont chargées les Autorités publiques ou à d'autres fins que celles pour lesquelles elles ont été collectées* ».

[12] Soit, selon l'article A.III.1.70) du Projet, « *mise à disposition ou transmission de données publiques entre Autorités publiques, aux seules fins de l'exercice de leurs missions de services publics ou de leurs obligations d'intérêt général, à l'exclusion des partages avec le CIRB dans sa fonction de gestionnaire de la Plateforme bruxelloise de la donnée par rapport au Catalogue des données et à l'exclusion des partages visant les données ouvertes, sans conditions de réutilisation, disponibles dans le Portail ouvert des données publiques de la Plateforme bruxelloise de la donnée* ».

[13] L'article A.III.1.80) du Projet définit l'intégration de données comme le « *processus de combinaison de différents jeux de données pour en créer un seul plus complet et plus cohérent* ». L'article A.III.1.12) du Projet définit le « jeu de données » comme « *ensemble cohérent de ressources ou d'informations (fichiers de données, fichiers d'explications, API, lien…) et de métadonnées (description, producteur, date de publication, mots-clefs, couverture géographique temporelle…) sur un thème donné* ».

[14] Soit, au sens de l'article A.III.1.86) du Projet, la « *capacité de différents systèmes, équipements, logiciels ou services à fonctionner ensemble de manière cohérente et à échanger des informations* ».

[15] « *Est un partenariat numérique de données toute initiative impliquant la valorisation ou le partage de données publiques et liant juridiquement ou administrativement, soit deux ou plusieurs entités au sein d'une même Autorité publique, soit deux ou plusieurs entités disposant de la personnalité juridique dont au moins une est une Autorité publique* », article C.III.2, § 1er, al. 2, du Projet. Le partenariat numérique peut être public ou mixte selon qu'il est conclu ou pas avec une autre autorité publique.

[16] Voir les considérants nos 74-75.

- Il **place une autorité publique incontournable, au cœur du traitement de données dans la Région de Bruxelles-Capitale** ;

- Sur **le plan conceptuel, il semble porter une certaine conception patrimoniale de la donnée** (à caractère personnel ou non) dont les conséquences concrètes sont floues.

13. Ces motifs méritent d'être étayés sur la base du dispositif et de l'exposé des motifs du Projet.

A) Facilitation du traitement des données, de leur circulation entre autorités et de leur concentration

14. Les éléments suivants indiquent clairement que le Projet s'inscrit dans une dynamique de facilitation du traitement de données à caractère personnel (le gras et soulignement sont ajoutés par l'Autorité dans les citations ci-après) :

- Au-delà du principe déjà connu en droit belge (fédéral et fédéré), du recours aux **sources authentiques** de données conservé dans le Projet, l'article C.II.3. de ce dernier, dédié au « ***Principe de partage*** » des données, prévoit en son paragraphe 1er que « *Par défaut, les Autorités publiques organisent le partage administratif de données entre elles afin d'améliorer l'exercice de leurs missions de services publics et de leurs obligations d'intérêt général, et, d'alléger le cas échéant la charge administrative des citoyens* » ; l'article C.IV.4 du Projet, intitulé « ***Partage administratif par défaut*** *et demande de partage administratif* » consacre le principe selon lequel les autorités partagent entre elles les données. L'exposé des motifs précise que « *le caractère gratuit du partage* [administratif] *se justifie par la* ***volonté de faciliter et d'encourager le partage de données entre Autorités publiques*** » ;

- Le Projet prévoit la possibilité de mettre en place des **bases de données issues de sources authentiques de données**, soit des **« *super bases de données* »** des termes mêmes de l'exposé des motifs ;

- Le Projet est tourné vers l'objectif de la **plus grande interopérabilité**, ainsi, « *Les Autorités publiques déploient des solutions qui privilégient les standards communs* »[17] et les « *Autorités*

[17] Article C.II.9 du Projet (il s'agit d'un « *objectif stratégique* » de la gouvernance de la donnée).

Sur l'adoption de standards communs, l'exposé des motifs énonce ce qui suit :

« *Le volume grandissant de données et le développement de leur utilisation présentent des risques importants de développement de modèles différents, dont la coexistence génère une baisse de l'efficacité de la gestion et une augmentation substantielle des coûts*.

publiques prennent toutes les mesures nécessaires (organisationnelles, juridiques et techniques) pour ***assurer l'interopérabilité*** *des données qu'elles détiennent et ce,* ***dès la conception*** *de leur processus*[, elles] *recourent à des systèmes interopérables qui s'appuient, chaque fois que cela est possible, sur des standards reconnus au niveau national ou international* »[18] ; *les données qu'elles détiennent « sont* ***intégrées dans des systèmes d'information interopérables****, tels que décrits à l'article C.II.17* »[19] ;

- Parmi les objectifs opérationnels assignés aux autorités dans le cadre de la gouvernance de la donnée, celles-ci doivent[20] « ***procéder à l'intégration de données*** [[21]] »[22], autrement dit leur centralisation/concentration ; le Projet prévoit que les « *autorités publiques* ***intègrent les données susceptibles de l'être*** »[23, 24] ;

- Les autorités publiques doivent identifier les **données de référence**[25] **et en favoriser l'usage**, y compris enfin de « *garantir, le cas échéant, le partage de données* »[26] ;

- « *La gouvernance numérique a pour objectif d'optimiser la cohérence et* ***la mutualisation*** *de* ***l'écosystème numérique bruxellois*** »[27], le Projet définissant ce dernier comme « *le réseau*

L'utilisation de standards communs pour la gestion des données favorise l'interopérabilité et facilite l'échange de données entre les différentes parties prenantes. Cela garantit également la cohérence, la qualité et la compatibilité des données, ce qui est essentiel pour assurer leur intégrité et leur utilisation efficace.

Pour garantir l'efficacité dans la gestion et optimiser les dépenses liées à la gestion et à l'utilisation des données, les Autorités publiques doivent donc favoriser l'utilisation de solutions mutualisées. Partager les coûts liés aux développements de nouvelles solutions permet de réaliser des économies d'échelles et d'accélérer la transformation « data ». Standardiser les outils et les échanges de données permettra également d'éviter de dupliquer les données, ce qui facilite le respect des principes de sécurité et le respect des droits individuels. Le partage de solutions et de standards communs d'architecture des données, permet également de travailler ensemble au développement des compétences communes » (souligné par l'Autorité).

[18] Article C.II.17 du Projet. Au sujet de **l'interopérabilité**, l'exposé des motifs précise ce qui suit :

« *Pour que les données puissent être valorisées, diffusées et échangées, comprises et réutilisées, il est nécessaire qu'elles respectent des règles d'interopérabilité. Il est donc nécessaire que les Autorités publiques mettent en place des systèmes interopérables entre eux en vue d'assurer le plus haut niveau de qualité des données.*

[…]

Cet objectif opérationnel préfigure l'application future du Règlement pour une Europe interopérable (actuellement proposition de Règlement du Parlement Européen et du Conseil établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union, COM(2022) 720 final, adoptée le 18 novembre 2022). Outre la question de l'interopérabilité elle-même, les Autorités publiques préparent ainsi leur participation aux « datas spaces » […] » (souligné par l'Autorité).

[19] Article C.III.16, al. 2, 3°, du Projet.

[20] La formulation de la disposition en projet est toutefois inhabituelle. Plutôt que d'exprimer une simple obligation à charge des autorités, elle dispose que « *Dans le cadre de leurs missions, les Autorités publiques s'engagent à* » (souligné par l'Autorité).

[21] Voir la note de bas de page n° 13.

[22] Article C.II.3, 6°, du Projet.

[23] Article C.II.19 du Projet.

[24] L'exposé des motifs précise que :

« *Cet objectif vise à ce que les Autorités publiques soient en mesure de combiner des données provenant de plusieurs sources d'origine afin de fournir aux utilisateurs une vue unifiée unique* » (souligné par l'Autorité).

[25] Voir la note de bas de page n° 7.

[26] Article C.II.20 du Projet.

[27] Article VI.2, § 1er, al. 1er, du Projet.

de parties prenantes, partenaires, infrastructures informatiques, systèmes d'informations qui sont interconnectés dans un espace numérique, ainsi que des réseaux de communication électroniques, filaires et radios, au sein du territoire de la Région de Bruxelles-Capitale »[28].

15. Or il ne fait pas de doute que la facilitation des traitements de données et de leur circulation entre autorités publiques telle qu'envisagée par le Projet, notamment par la concentration des données et de leurs moyens de traitement, toutes finalités confondues, présente un risque élevé pour les droits et libertés des personnes concernées : sans préjudice des développements ultérieurs, **sa nécessité et sa proportionnalité doivent tout d'abord être démontrées, et les garanties appropriées contre les risques pour les droits et libertés des personnes concernées doivent être déterminées et mises en évidence**[29]. L'Autorité rappelle au passage qu'il convient « *de souligner que le manque de ressources allouées aux autorités publiques ne saurait en aucun cas constituer un motif légitime permettant de justifier une atteinte aux droits fondamentaux garantis par la Charte* »[30].

B) Le CIRB (PARADIGM), une institution centrale et incontournable du traitement de données

16. Le **CIRB** (« **Centre d'informatique pour la Région Bruxelloise** »), plus récemment renommé « **Paradigm** »[31], apparaît comme **l'institution centrale au traitement de données** dans la Région de Bruxelles-Capitale (sa nouvelle dénomination « *Paradigm* » est édifiante à cet égard). Il s'agit d'un organisme d'intérêt public institué par l'article 27 de la loi *du 21 août 1987 modifiant la loi organisant les agglomérations et les fédérations de communes et portant des dispositions relatives à la Région bruxelloise*, jouissant de la personnalité civile, dont la gestion journalière est assurée par un fonctionnaire dirigeant et un fonctionnaire dirigeant adjoint désignés par le Gouvernement de la Région

---

[28] Article A.III.1.46) du Projet.

[29] Dans son **avis n° 1/2023 du 13 janvier 2023** ***concernant la proposition de règlement pour une Europe interopérable*****, le Contrôleur européen de la Protection des Données** rappelle en synthèse que :

« *Le CEPD reconnaît les avantages qui peuvent découler d'une interopérabilité accrue dans le secteur public et salue les efforts consentis par la Commission pour organiser et institutionnaliser le processus dans ce sens. Cependant,* ***le CEPD rappelle également que l'interopérabilité des réseaux et des systèmes d'information dans tous les secteurs de l'administration publique et à tous les niveaux de l'administration compromet l'un des principes les plus fondamentaux de la protection des données, à savoir le principe de la limitation des finalités****. Il est dès lors* ***essentiel*** ***que les risques créés par l'élimination des obstacles techniques à l'échange d'informations soient examinés de façon plus approfondie*** ***dans le processus*** » (gras ajouté et souligné par l'Autorité).

Il souligne encore au considérant n° 7 du même avis, ce qui suit :

« *le CEPD rappelle qu'un* ***environnement technologique avec des systèmes d'information qui ne sont pas interopérables entre eux a offert une grande protection contre la violation de l'un des principes fondamentaux de la protection des données, à savoir le principe de la limitation des finalités****. Bien qu'une interopérabilité insuffisante ne soit pas une mesure technique délibérée afin de garantir un traitement licite, celle-ci s'est révélée* ***efficace pendant des décennies****. La non-faisabilité technique a rendu plus difficile l'utilisation de grandes quantités de données pour des finalités autres que celles pour lesquelles elles ont été collectées.* ***L'élimination de cet obstacle technique nécessite une prise en considération accrue des limitations juridiques*** *et pourrait également garantir de nouvelles mesures de protection afin de veiller à la licéité du traitement et de la reddition de comptes* » (gras ajouté par l'Autorité).

[30] CJUE (Gr. Ch.), arrêt du 1er août 2022, *OT c/ Vyriausioji tarnybinės etikos komisija*, aff. C-28/08, considérant n° 89.

[31] Voir https://paradigm.brussels/fr/paradigm/base-legale-du-cirb, dernièrement consulté le 2 octobre 2023. A la connaissance de l'Autorité, l'avant-projet d'ordonnance relatif à Paradigm et qui a donné lieu à l'avis standard de l'Autorité lors de sa séance du 8 septembre 2023 n'a pas encore été voté.

de Bruxelles-Capitale. Le CIRB (PARADIGM) semble dépendre d'un Ministre de tutelle (*a priori*, le demandeur)[32].

17. **Le Projet illustre abondamment le rôle central et incontournable du CIRB (PARADIGM) dans tous les domaines du traitement de données dans l'ordre juridique public bruxellois :** réalisation des traitements, infrastructure, choix technologiques, expertise, etc.). Plus concrètement, le Projet attribue ainsi les missions suivantes au CIRB (PARADIGM) (le gras est ajouté par l'Autorité dans les citations ci-après) :

- Le CIRB (PARADIGM) « *est chargé de* ***l'opérationnalisation et de la mise en œuvre des sites internet*** *qui composent l'écosystème web bruxellois* »[33] ;

- Les autorités publiques **doivent collecter les données issues de sources authentiques auprès du** Centre d'intégration de la Plateforme bruxelloise de la donnée[34]. Cette **plateforme** est instituée au sein du **CIRB (PARADIGM)** et le CIRB (PARADIGM) en est le « *gestionnaire* »[35]. Il assure notamment dans ce cadre, « *l'administration technique de la Plateforme, notamment en ce qui concerne l'infrastructure, la sécurité, la gestion ou la disponibilité des informations ou, le cas échéant, des données* » ; « *le cas échéant, le contrôle des schémas d'identification électronique ou de la certification au sens du Règlement (UE) No 910/2014 (EIDAS)* » ; « *Le cas échéant, la désignation d'un prestataire indépendant en qualité de tiers de confiance* » ; « *le conseil et l'assistance aux Autorités publiques utilisatrices ainsi que la coordination avec leurs représentants, notamment en ce qui concerne la formation à l'utilisation, la prise en charge de projets particuliers, ou tout autre domaine pertinent en relation avec l'utilisation de la Plateforme ; la conception évolutive de l'architecture de la Plateforme conformément à la stratégie pluriannuelle de la donnée ainsi que les plans d'actions annuels, visés à l'article C. VI.15, § 2* »[36] ;

- Le CIRB (PARADIGM) (comme intégrateur de service), notamment, peut **demander qu'une source de données soit désignée** comme source authentique[37] ;

---

[32] «Dans l'exercice de ces compétences, Paradigm joue un rôle d'appui au Ministre de tutelle en charge de l'Informatique et de la Transition numérique », voir https://paradigm.brussels/fr/paradigm, dernièrement consulté le 06/10/2023.

[33] C'est-à-dire, les sites dont le nombre et les modalités sont définis par le Gouvernement, le Collège réuni et le Collège. Voir l'article B.I.5, al. 2, du Projet.

[34] Voir les articles, C.II.3, § 2, al. 2, et C.IV.12, § 2, du Projet.

[35] Article C.V.1, §§ 1er et 2, du Projet.

[36] Voir l'article C.V.2 du Projet.

[37] Article C.IV.15, § 2, 1°, du Projet.

- Les services offerts via cette plateforme sont accessibles sur la base d'un « ***accord d'adhésion*** » entre le CIRB (PARADIGM) et l'utilisateur de la plateforme[38] ; et c'est le gestionnaire de la plateforme (le CIRB (PARADIGM)) qui est chargé de « *l'établissement du cadre documentaire de base et d'accord d'adhésion permettant son utilisation, notamment en ce qui concerne les formalités ou les modalités d'adhésion à la Plateforme et d'utilisation de ses services* […] »[39] ;

- **En principe, tout échange de données avec une autorité publique bruxelloise doit passer par le CIRB (PARADIGM)**. Ainsi, « *Tout partage administratif* [[40]] *est réalisé au travers du Centre d'intégration, en l'absence de législation particulière organisant spécifiquement le partage administratif visé* »[41] (souligné par l'Autorité), règle valant également, en l'absence de disposition légale ou réglementaire contraire, pour l'échange de donnée entre autorité publique et « ***autorités publiques tierces*** »[42] (c.-à-d., fédérale ou autre, et même internationale[43])[44]. Dans le cas où les données sont partagées administrativement avec une autorité tierce, l' « *intégrateur de services bruxellois* »[45] doit aussi vérifier que les autorisations nécessaires ont été obtenues avant de permettre le partage administratif[46]. C'est via le « *Centre d'intégration* » que le CIRB (PARADIGM) **assure techniquement les partages administratifs**[47] ;

- Le CIRB (PARADIGM) est responsable de l'organisation de **l'altruisme en matière de données[48]** ;

---

[38] Voir l'article C.V.3 du Projet.

[39] Voir l'article C.V.2, al. 1er, 3°, du Projet.

[40] Voir la note de bas de page n° 12.

[41] Article C.IV.5, § 1er, du Projet.

[42] Voir la note de bas de page n° 2.

[43] Voir la note de bas de page n° 2.

[44] « *Dans ces hypothèses, le partage administratif est réalisé au travers du Centre d'intégration et, le cas échéant, le Centre d'intégration le relais obligatoire entre les Autorités publiques et les autres intégrateurs de services des Autorités publiques tierces* », article C.IV.5, § 2, al. 1er, du Projet.

[45] Soit, selon l'article A.III.1.102) du Projet, « *l'institution désignée à l'article C.V.7* ». Selon l'article C.V.7, le Centre d'intégration est créé au sein de la Plateforme bruxelloise de la donnée. C'est l'article C.V.8 du Projet qui prévoit que « *Le CIRB (PARADIGM) est désigné en qualité d'intégrateur de services bruxellois dans le cadre de sa gestion du Centre d'intégration* ». **Le Projet doit par conséquent être adapté sur ce point**.

[46] Article C.IV.5, § 2, al. 2, du Projet

[47] Voir l'article C.V.7 du Projet.

[48] Voir l'article C.IV.33 du Projet.

- Le CIRB (PARADIGM) offre les services que constituent le **Catalogue des données**[49], le **Portail ouvert des données publiques** qui « *propose les données disponibles à la réutilisation* »[50] et le « **Centre d'exploitation et d'analyse des données** »[51] ;

- Le CIRB (PARADIGM), en tant qu'intégrateur de services bruxellois, notamment, procède « *au **partage administratif de données intégrées** à la demande de l'Autorité publique destinataire* », ce qui laisse entendre que les données sont intégrées auprès du CIRB (PARADIGM) lui-même ; et le CIRB (PARADIGM) peut « *développer pour les services publics participants des **applications utiles à l'échange et/ou l'intégration de données** conservées dans les banques de données* »[52] ;

- C'est aussi à la plateforme bruxelloise de la donnée que sont intégrés les **services d'appui** (et d'assistance) visés à l'article 7 du Règlement sur la Gouvernance des Données, le CIRB (PARADIGM) constituant autrement dit, un organisme compétent au sens de cette disposition[53] ;

- Le **CIRB (PARADIGM) se trouve encore au cœur des « *organes de la gouvernance* » mis en place par le Projet**. Ainsi, le **Secrétariat numérique** est créé au sein du CIRB (PARADIGM)[54]. Le CIRB (PARADIGM) assure de la sorte le secrétariat du Comité de coordination numérique et du Comité de validation de l'architecture numérique.

  Le **Comité de validation de l'architecture numérique** est notamment « *responsable de la gouvernance de l'architecture numérique régionale à des fins de cohérence et de mutualisation* »[55].

  Le **Bureau d'achats numériques** est créé au sein du CIRB (PARADIGM). Dans ce cadre notamment, le CIRB (PARADIGM) « *fournit tout appui opérationnel, légal ou technique, aux Autorités publiques* » « *concernant les processus de commande publique numérique mutualisable* »[56] ; il est notamment compétent pour fournir une assistance nécessaire à toute autorité publique dans le cadre de tout processus de commande publique numérique mutualisable susceptible d'affecter l'écosystème numérique bruxellois ; il propose au

[49] Voir l'article C.V.9 du Projet.
[50] Voir l'article C.V.10 du Projet.
[51] Voir l'article C.V.11 du Projet.
[52] Voir l'article C.V.8 du Projet.
[53] Voir l'article C.V.13 du Projet.
[54] Voir l'article V.VI.4 du Projet.
[55] Voir l'article C.VI.6 du Projet.
[56] Article C.VI.8 du Projet.

Gouvernement « *les critères de mutualisation pertinents en matière de commande publique numérique* », il remet des avis sur les projets soumis au test d'autoévaluation numérique ; il remet d'initiative ou à la demande « *des avis* » au Comité de validation de l'architecture numérique, au Comité de coordination numérique et au Bureau de la donnée[57]. Le Comité de coordination numérique « *se prononce stratégiquement sur tous les projets visés à l'article C.VI.3, § 2, soumis au test d'autoévaluation numérique* » préalablement analysés par tout ou partie des organes consultatifs et remet lui-même des avis à ce sujet[58] ; il peut aussi émettre des avis d'initiative ou à la demande[59] ;

Le **Bureau de la donnée** est créé au sein du CIRB (PARADIGM)[60]. Notamment, en concertation avec le Comité de Gouvernance de la donnée, il appuie et anime le Comité de gouvernance de la Donnée, il rédige des avis d'initiative ou à la demande, il a une mission de « *coordinateur de la donnée, avant validation par le Comité de gouvernance de la donnée, notamment au travers de* […,] *l'organisation d'un cadre pour la gestion de l'interopérabilité* », il a une « *mission d'accompagnement à la mise en œuvre des obligations du Code en matière de gestion de la donnée notamment au travers de* […] *la proposition de directives, de standards, de cadres et de lignes directrices à faire approuver par le Comité de gouvernance de la donnée* », au travers de « *la promotion d'instruments de politiques internes aux Autorités publiques concernant la gestion des données au sens du chapitre 1 du titre 4 du livre C.III, en ce compris la gestion des modèles analytiques, des algorithmes et des systèmes exploitant l'intelligence artificielle au sens de l'article C.III.18* », il a encore une mission « *d'initiateur du changement au travers de a) la mise en place de communautés de pratiques* […] », une « *mission de support au travers de la mise à disposition d'experts en gouvernance de la donnée lorsque les autorités publiques ne disposent pas des ressources suffisantes* »[61]. Le Bureau de la donnée est « *placé sous la responsabilité d'un coordinateur de la donnée* » et ses objectifs stratégiques sont définis par le « *Ministre compétent à l'égard du CIRB et les Ministres compétents en matière numérique du Collège réuni et du Collège* »[62].

Le CIRB (PARADIGM) fait partie de la composition du **Comité de gouvernance de la donnée**[63] qui notamment, fixe « *les objectifs opérationnels du Bureau de la donnée* » (le CIRB (PARADIGM) de nouveau), revoit et valide les « *standards, bonnes pratiques et modèles soumis pour proposition par le Bureau de la Donnée, notamment en matière*

[57] Article C.VI.9 du Projet.

[58] Voir l'article C.VI.11 du Projet.

[59] *Ibid.*

[60] Article C.VI.17 du Projet.

[61] Article C.VI.18 du Projet.

[62] Article C.VI.19 du Projet.

[63] Voir l'article C.VI.14 du Projet.

d'interopérabilité », a pour objectif « *de s'assurer de l'opérationnalité des dispositions du Code en se concentrant sur l'ensemble des points nécessitant des responsabilités claires, notamment la désignation de commun accord de l'identité de la ou des Autorités publique investies de la responsabilité de la gestion d'un domaine spécifique de données* »[64].

- Le CIRB (PARADIGM) « *est chargé de la mise en place du* ***réseau bruxellois de fibre optique*** ***mutualisant les réseaux de fibre optique*** *dont disposent certaines Autorités publiques sur le territoire régional bruxellois. Dans ce cadre, le CIRB désigne une entité chargée des missions* » décrites par le Projet[65]. Et en ce qui concerne ce réseau de fibre optique bruxellois, « *Les Autorités publiques disposant d'un réseau de fibre optique concluent avec l'entité désignée* […] *et le CIRB une convention arrêtant notamment toute modalité technique, opérationnelle et financière des missions* » listées par le Projet[66] ;

- Enfin, c'et encore le CIRB (PARADIGM) qui, dans le Titre 3 du Projet, « *chargé de la* ***collecte, de la validation, de l'enregistrement, du stockage, de la mise à jour et de la mise à disposition des données*** *contenues dans la banque de données issues de sources authentiques* ***Brussels UrbIS*** », et est désigné comme « ***gestionnaire de la banque de données Brussels UrbIS*** »[67] qui comprend une série importante de catégories de données géographiques au sujet de la Région de Bruxelles-Capitale[68], et offre notamment la possibilité de superposer les informations géographiques et, de connaître les coordonnées géographiques de n'importe quel lieu et d'échanger des données pouvant être reliées à Brussels UrbIS[69].

18. En outre, au-delà du Projet, en droit positif, il convient encore de souligner que :

- **Le CIRB (PARADIGM) est le gestionnaire de la plateforme bruxelloise de vidéoprotection** (soit la plateforme de mutualisation des images et données collectées à partir des caméras de surveillance), **dont il est aussi membre du Comité stratégique**[70]. Il est compétent « *pour la gestion des aspects juridiques liés au fonctionnement de la plate-*

[64] Voir l'article C.VI.15 du Projet.

[65] Article C.VI.24, § 1er, du Projet, intitulé « *La gestion des réseaux de fibre optique publics* ».

[66] Article C.VI.24, § 5, du Projet.

[67] Article 6 du Titre III du Projet.

[68] Dont les noms des communes et des rues, numéros de police et boîtes, bâtiments extraits des permis d'urbanisme, emplacements, situation de fait et de droit pour toutes ces données, parcelles cadastrales, adresses, et les liaisons entre certaines données, dont « *les liaisons entre d'une part les adresses et d'autre part, les bâtiments, unités de bâtiments, parcelles, emplacements et postes d'amarrage* ». Voir l'article 10 du Titre III du Projet.

[69] Voir l'article 5 du Titre III du Projet.

[70] Voir l'article 2, 12°, de l'Ordonnance du 28 mai 2015 *créant un organisme d'intérêt public centralisant la gestion de la politique de prévention et de sécurité en Région de Bruxelles-Capitale et créant l'Ecole régionale des métiers de la sécurité, de la prévention et du secours – Brusafe*.

forme bruxelloise de vidéoprotection, des aspects techniques liés au fonctionnement du système de mutualisation d'images et de données ainsi que pour la gestion des achats »[71] ;

- Et c'est enfin encore le CIRB (PARADIGM) qui gère « IRISbox », soit « *Le* ***guichet électronique des administrations de la Région bruxelloise*** », « *qui propose des services régionaux et locaux en ligne* », auxquels « *citoyens et entreprises y consultent 24h sur 24 et 7 jours sur 7 des documents en ligne et ont accès à des formulaires interactifs pour demander les documents et effectuer des démarches administratives* »[72].

19. Or de nouveau, il est tout aussi clair que l'attribution de toutes ces compétences et pouvoirs à une seule et même institution présente des risques élevés pour les droits et libertés des personnes concernées. Une fois de plus, **sans préjudice des développements ultérieurs, la nécessité d'une telle centralité et sa proportionnalité doivent tout d'abord être démontrées, et les garanties appropriées contre les risques pour les droits et libertés des personnes concernées doivent être déterminées et mises en évidence**. Dans ce contexte, il est particulièrement important de **déterminer et prendre en compte la responsabilité des diverses entités concernées**[73].

C) Une certaine conception patrimoniale de la donnée aux conséquences concrètes floues

20. Enfin, **sur le plan conceptuel, le Projet semble privilégier une vision patrimoniale focalisée (ou axée) sur la donnée plutôt que sur la personne concernée** ou le citoyen destinataire des missions de service public concernées ainsi que sur ces dernières, **sans que les conséquences concrètes d'une telle approche n'apparaissent clairement,** à tout le moins sur le plan du traitement de données à caractère personnel. En ce sens :

- L'article C.II.7. du Projet, prévoyant un « *Objectif stratégique* » de la gouvernance de la donnée « *Approche centrée sur la donnée* », s'énonce comme suit : « *Les Autorités publiques adoptent des processus qui* ***placent les données au centre*** *de la gestion de leurs missions de services publics et de leurs obligations d'intérêt général, de même que de leur*

[71] Voir l'article 10/9, § 2, de l'ordonnance citée à la note de bas de page n° 70. L'Autorité souligne en passant, bien qu'elle ne se prononce pas en l'occurrence au sujet de cette ordonnance, que la désignation des responsabilités au regard du traitement de données à caractère personnel dans le cadre de cette dernière n'est pas conforme à la pratique de l'Autorité (voir les considérants nos 167 et s.).

[72] Voir https://irisbox.irisnet.be/irisbox/about, dernièrement consulté le 06/10/2023. Selon les conditions générales d'utilisation d'IRISbox, « *Le présent portail Internet est une initiative de Paradigm, parastatal « A » créé par l'article 27 de la loi du 21 août 1987 modifiant la loi organisant les agglomérations et les fédérations de communes et portant des dispositions relatives à la Région Bruxelloise, dont le siège social est établi avenue des Arts 21, 1000 Bruxelles* » ; « *Pour le site internet IRISbox, le responsable de traitement est le Centre d'Informatique pour la Région Bruxelloise dont le siège social est établi avenue des Arts 21, 1000 Bruxelles* » (ce qui pour le reste, n'est pas clair quant au « portail Internet » et aux services offerts via IRISbox (p. ex., demandes de documents auprès des communes, extraits de casier judiciaire, etc.).

[73] Voir les considérants nos 167 et s.

gouvernance. Les données des Autorités publiques ***sont assimilées à des actifs à part entière*** »[74] (souligné par l'Autorité). L'exposé des motifs évoque un « ***nouveau paradigme où la donnée devient centrale*** », précise que l'approche centrée sur la donnée permet aux autorités de faire de la gouvernance des données une priorité « *notamment en donnant la priorité à des outils performants et puissants, par exemple pour accéder, stocker ou protéger les données en interne ou de manière externe* », ce qui permet de « ***maximiser la valeur des données*** *en les utilisant de manière pertinente et stratégique* » ;

- Parmi les objectifs opérationnels assignés aux autorités dans le cadre de la gouvernance de la donnée, celles-ci doivent[75] « ***valoriser leurs données****, le cas échéant en fonction de leurs priorités* »[76] ; et « *Afin d'identifier les ressources numériques dont elles disposent et qu'il leur appartient de* ***valoriser****, les Autorités publiques identifient les partenariats numériques*[77] *de données dont elles sont parties* »[78] ; « *La valorisation des données détenues par les Autorités publiques vise à organiser la gestion des données* ***en tant que sources de valeur et véritables actifs numériques*** »[79] ; la valorisation des données repose notamment sur la valorisation des données d'usage[80] ; l'article C.III.10 du Projet prévoit que les données appartiennent à des catégories « *en fonction de leur régime de* ***propriété*** » ; les autorités doivent définir une « ***stratégie de valorisation*** » des données dans le cadre de leurs missions et obligations[81] ;

- Le Projet porte également sur les « ***partenariats numériques*** », à ce sujet, l'exposé des motifs énonce que « *Cette notion a pour seule ambition de permettre aux Autorités publiques de qualifier les liens juridiques ou administratifs qu'elles entretiennent* ***et dont la finalité est la valorisation de données*** »[82]. Le Projet est centré à cet égard sur la valorisation de la

---

[74] Sur l'identification des données comme actif, voir la note de bas de page n° 82, dernière citation.

[75] Voir la note de bas de page n° 20.

[76] Article C.II.3, 1°, du Projet.

[77] Voir la note de bas de page n° 15.

[78] Article C.III.2, § 1er, al. 1er, du Projet.

[79] Article C.III.11 du Projet.

[80] Voir la note de bas de page n° 6 concernant la définition de donnée d'usage.

[81] Voir l'article C.II.14 du Projet. L'exposé des motifs précise que « *Cet objectif vise à reconnaître la valeur potentielle des données détenues par une Autorité publique et à déterminer les priorités en termes d'utilisation et de valorisation* » (souligné par l'Autorité).

[82] Il précise encore ce qui suit :

« *Actuellement, les Autorités publiques ignorent trop souvent quelles données elles détiennent et de quelle manière le traitement de ces données pourrait, non seulement, leur permettre de réaliser leurs missions de service public ou leurs obligations d'intérêt général avec plus d'efficience, mais également, par ailleurs parvenir à intéresser également les autres Autorités publiques, les collectivités publiques du pays ou encore des opérateurs socio-économiques* » (souligné par l'Autorité).

« […] *les Autorités publiques vont être amenées, étape par étape, à identifier parmi les données détenues celles qui seront susceptibles de créer de la valeur et de quelle manière ces données peuvent être valorisées* » (souligné par l'Autorité).

Ailleurs, l'exposé des motifs exprime ceci :

« *il faut comprendre que la valorisation vise l'enrichissement, le renforcement ou l'amélioration des connaissances relatives aux données existantes de manière à leur conférer une certaine valeur. Cet avantage pourrait, entre autres, être un avantage*

donnée **sans toutefois illustrer concrètement ce dont il est question et ce que cela implique, sous réserve des trois exemples suivants** : les cas de « *partages administratifs* », de « *réutilisation* » ou encore de « *communication* » sont les seules opérations de valorisation et de partage de données très spécifiques régies par le Code et juridiquement encadrées[83].

21. D'emblée dans ce contexte, **l'Autorité souligne que la valorisation des données au sens du Projet ne constitue pas en elle-même, une finalité de traitement déterminée**. Autrement dit, cet objectif porté par le Projet ne pourra à lui seul, fonder un traitement de données à caractère personnel. L'Autorité rappelle aussi que s'agissant du traitement de données à caractère personnel,

économique, en l'espèce numérique. Les objectifs liés à un projet de valorisation de données sont très variés et dépendent du champ d'application concerné.

Par la valorisation des données, les Autorités publiques vont faire des données de véritables biens publics concourant à l'amélioration de l'efficacité de leurs services et de la mise en œuvre de leurs missions. A ce jour, beaucoup d'Autorités génèrent des données, sans avoir conscience de la valeur qu'elles possèdent. Cette méconnaissance du patrimoine numérique bruxellois peut aboutir à des opportunités manquées et engendrer des pertes financières (par ignorance des traitements qui peuvent être mutualisés par exemple) ou par la mise en cause de responsabilités à la suite de fuites de données insuffisamment sécurisées, faute de prise en considération de leur importance ou de leur sensibilité.

Le titre 3 a pour objectif de permettre aux Autorités publiques d'augmenter leur capacité à adapter et mettre en place des solutions en partant des données dont elles disposent ou pourraient disposer. Dans ce cadre, les Autorités publiques doivent adopter une démarche de résolution de problèmes à l'aide de données.

Les Autorités publiques sont invitées à investir dans la création de processus, de compétences et de ressources leur permettant de mieux valoriser leurs données.

[…]

« *Cette classification devra également permettre la mise en place d'une architecture dite DATA CENTRIC.*

De manière théorique, on peut noter que la valorisation des données peut revêtir différentes formes. La doctrine distingue par exemple (voir à cet égard L.-D., Benyayerd, S., Chignard, Datanomics,FYP Editions, Paris, p.49):

1° « quand elles sont revendues par ceux qui les collectent ou les agrègent, les données prennent une forme de matière première.

2° quand elles sont utilisées sans marchandisation, par exemple pour réduire des coûts ou développer les revenus, elles prennent une forme de levier.

3° quand elles constituent une arme stratégique pour défendre ou conquérir une position concurrentielle, elles prennent une valeur d'actif. »

Dans le cas des Autorités publiques, la majorité des cas de valorisation se rapportent à la mise en place de leviers. Les données détenues par les Autorités publiques seront notamment et principalement utilisées et partagées pour :

1° prendre de meilleures décisions et réduire les coûts de fonctionnement des Autorités publiques ;

2° offrir de meilleurs ou de nouveaux services aux citoyens.

Il ne faut pas pour autant oublier que les données produites par les Autorités publiques peuvent être utilisées par des opérateurs privés pour d'autres types de valorisation.

L'objectif est donc au minimum double :

1° permettre une meilleure gestion interne des services publics et des obligations d'intérêt général des Autorités publiques, par une meilleure valorisation des données ; identifier les données qu'une Autorité publique possède lui permettra d'optimiser ses process internes et sa relation avec ses administrés, de sécuriser davantage les données et d'augmenter la confiance qui en découle,

2° *permettre de véritables partages de données dans le cadre de réutilisations ou entre Autorités publiques (open data/réutilisation de données protégées ou application du once only) grâce à une meilleure gestion interne des données prêtes à l'usage pour d'autres Autorités publiques ou tout opérateur économique intéressé. La déclaration de principe permettra de mettre en place les bases (métadonnées et données de références) de ce qui constitue le Catalogue des données de la Plateforme bruxelloise de la donnée (voir le livre B.V).* » (souligné par l'Autorité).

[83] Il y aurait aussi partenariat numérique lorsque des autorités publiques décident de « *mutualiser certains outils, voire certaines compétences ou certains postes* », par exemple, « *un projet de mutualisation des données relatives à un territoire intelligent qui peut concerner des infrastructures numériques comme les réseaux de télécommunication, les centres d'hébergement ou des plateformes de traitement des données dédiées à un domaine spécifique (mobilité, agriculture, occupation territoire,…)* » (?).

une donnée à caractère personnel ne peut être considérée en faisant abstraction de la finalité pour laquelle elle est traitées et plus généralement, des règles régissant son traitement. Par définition en outre, une valorisation ne peut découler d'un fait illicite (soit en l'occurrence, un traitement de données qui ne serait pas conforme au RGPD) .

22. Ensuite, l'Autorité est d'avis qu'il est nécessaire **d'identifier clairement <u>l'impact de cet objectif de valorisation sur le traitement de données à caractère personnel</u>**, ainsi que les éventuels **<u>risques</u> qu'il présente pour les droits et libertés des personnes concernées <u>et les mesures prises</u> pour mitiger ceux-ci**. Sur ce point plus fondamentalement, **le demandeur doit s'interroger sur la plus-value du recours à un concept tel que celui de la valorisation et les conséquences conceptuelles qu'il y attache**, si ce dernier se limitait *in concreto*, à se référer en d'autres termes, à l'exécution par une autorité publique de sa mission d'intérêt public ou de ses obligations légales. La nouveauté portée par le Projet dans l'ordre juridique bruxellois doit être identifiée, tout comme son impact sur les droits et liberté des personnes concernées.

<u>II.1.3. Commentaires généraux concernant le Projet</u>

23. Les développements précédents appellent la formulation des trois commentaires généraux suivants.

24. **Premièrement**, conformément à sa pratique d'avis constante, l'Autorité rappelle que dans le cadre d'un traitement impliquant une **<u>ingérence importante dans les droits et libertés des personnes concernées</u>**, l'Autorité considère qu'en vertu de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la CEDH et 6.3 du RGPD, une norme de rang législatif doit déterminer dans quelles circonstances un traitement de données est autorisé. Conformément au principe de légalité, cette norme législative doit ainsi, en tout cas, fixer les éléments essentiels du traitement. Lorsque le traitement de données constitue une ingérence particulièrement importante dans les droits et libertés des personnes concernées, comme c'est le cas en l'espèce, il est nécessaire que les éléments essentiels suivants soient déterminés par le législateur : la (les) finalité(s) précise(s)[84] à la lecture de laquelle (desquelles) on peut déjà apercevoir les traitements de données qui seront mis en place pour sa (leur) réalisation, l'identité du (des) responsable(s) du traitement (si c'est déjà possible), les (catégories de) données qui sont nécessaires à la réalisation de cette (ces) finalité(s), le délai de conservation des données, les catégories de personnes concernées dont les données seront traitées, les (catégories de) destinataires auxquels les données seront communiquées, les circonstances dans lesquelles elles seront communiquées ainsi que l'éventuelle limitation des obligations et/ou des droits visé(e)s aux articles 5, 12 à 22 et 34 du RGPD.

[84] Voir aussi l'article 6, 3., du RGPD.

25. En l'occurrence, compte-tenu de la portée du Projet, **celui-ci devra en principe généralement être lu concomitamment avec le cadre normatif régissant les missions et obligations des autorités publiques concernées**. Autrement dit dans plusieurs hypothèses, par exemple s'agissant de l'échange de données entre autorités publiques, le Projet ne peut à lui seul fonder juridiquement le traitement de données à caractère personnel.

26. **Deuxièmement**, compte-tenu des très nombreuses relations existant entre le Projet et les règles de protection des données (le Projet contient des règles sur la classification des données, les recours, les analyses de risque, les responsabilités, la sécurité de l'information, la conformité, la traçabilité et la responsabilités des autorités publiques, la correction des données, etc.), du fait que le Projet soit une *lex posterior* du rang de loi, et du fait que le RGPD laisse une marge de manœuvre aux Etats Membres à plusieurs égards, en particulier s'agissant du traitement de données dans le secteur public, **l'Autorité est d'avis qu'une disposition générale devrait spécifier que le Projet est sans préjudice du RGPD et ne peut être lu comme limitant les droits des personnes concernées ou les obligations du responsable du traitement**.

27. **Troisièmement**, l'Autorité déplore que le Projet n'ait pas fait de la part du demandeur, l'objet d'une analyse d'impact. Elle est d'avis qu'**un Projet d'une telle ambition[85] doit être accompagné d'une analyse d'impact qui adresse notamment la préoccupation générale juste exprimée par l'Autorité** (en particulier, voir les considérants nos 15, 19, 21 et 22 du présent avis). En l'occurrence, l'absence d'une telle analyse d'impact complique significativement la bonne appréhension des ambitions et de la portée du Projet. **L'Autorité est d'avis qu'une telle analyse est nécessaire en vue de l'organisation d'un débat parlementaire efficace**, au sujet des éléments du Projet concernant le traitement de données à caractère personnel. L'Autorité rappelle que conformément notamment à l'article 23 de la LTD, **cette analyse d'impact ne dispensera pas les responsables du traitement concernés** (à tout le moins, le CIRB/PARADIGM) de réaliser leurs propres analyses d'impact relatives à la protection des données en exécution de l'article 35 du RGPD.

---

[85] Au-delà des développements précédents, l'Autorité relève que le changement de paradigme apporté par le Projet serait justement également lié à la mise en conformité au RGPD. Notamment, l'exposé des motifs précise ce qui suit :

« *La mise en place d'une telle gouvernance est aussi l'occasion de passer d'un modèle « task centric » à un modèle « data centric » afin de fluidifier l'échange de l'information au sein de l'administration et donc de l'ensemble des processus métier. Autrement dit, mettre en œuvre une bonne gouvernance et architecture des données et des systèmes d'information peut être le moyen de faire un saut qualitatif majeur permettant de mieux rendre le service aux usagers, d'améliorer l'efficience en rationalisant les coûts et de se conformer sur l'exigence la plus difficile à rencontrer du RGPD : la privacy by design* ».

Il souligne encore les gains de qualité des données qui résulteraient de la nouvelle approche suggérée et aussi les réductions de coûts y liées : la démarche entreprise « *engendre un retour sur investissement non négligeable, contrairement à une approche par la pure conformité qui ne fait que coûter. Une telle démarche a un double avantage : premièrement d'apporter structurellement à l'administration une très grande part de la conformité avec un minimum de dépenses spécifiques pour le RGPD, et deuxièmement, d'amener un changement plus facile à initier puisqu'il se veut positif contrairement à une démarche conformiste qui implique généralement un changement sous contraintes* ».

Et encore : « *Entrer dans une telle démarche systémique alliant agilité, culture de la confiance et gouvernance des données, c'est intégrer totalement le principe qui nous semble plus important du PbD [(Privacy by design)] d'Ann Kavoukian : « full fonctionnality – Posistive-Sum, not Zero-sum* »[(« *A. BEELEN (dir.), La protection des données pour les institutions publiques, Anthemis, Limal, 2020, p/.229-230* »)] ».

II.2. TRANSPARENCE ADMINISTRATIVE

II.2.1. Publicité passive et intérêt

28. Selon l'article B.I.16, § 3, du Projet, « *Pour les documents administratifs contenant de l'information se rapportant à une personne physique identifiée ou identifiable, lorsque cette information constitue une appréciation ou un jugement de valeur relatif à cette personne ou lorsqu'elle se rapporte à un comportement de cette personne dont la divulgation peut manifestement lui causer préjudice, le demandeur doit justifier d'un intérêt* » (souligné par l'Autorité).

29. Autrement dit, dans les hypothèses ou d'autres données à caractère personnel sont consultées, le demandeur **ne** doit **pas** justifier d'un intérêt.

30. « *Sur le plan de la finalité et des (catégories de) données concernées, l'Autorité attire l'attention du demandeur sur le fait que l'accès à des données à caractère personnel* ***nécessitera généralement une balance des intérêts en présence et en tout cas, la prise en compte de la finalité (de l'intérêt) poursuivi par le demandeur concerné*** *et celle de la législation concernant l'accès en cause. Que cette balance soit réalisée via la réglementation (publicité active) ou in concreto sur la base de demandes individuelles ou en tout cas, d'accès conditionnés à l'information (publicité passive). L'Autorité a rappelé et explicité ces principes également, mutatis mutandis, aux considérants nos 15 à 22 de son avis n° 102/2020 du 19 octobre 2020 relatif à une demande d'avis concernant un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale modifiant l'arrêté du Gouvernement de la Région de Bruxelles Capitale du 25 avril 2019 réglant la forme ainsi que les procédés d'information et de mise à disposition des décisions prises en matière de permis d'urbanisme, de permis de lotir et de certificat d'urbanisme par le collège des bourgmestre et échevins, le fonctionnaire délégué et le Gouvernement* » (gras ajouté par l'Autorité dans le présent avis)[86].

31. Par conséquent[87], et compte-tenu du fait qu'en application de l'article 86 du RGPD, il appartient au droit national de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel au titre du RGPD, l'Autorité est d'avis que **l'article B.I.16, § 3, du Projet doit être adapté afin de garantir que,** sans préjudice d'une norme du rang de loi prévoyant un accès libre et inconditionné du grand public aux documents concernés, **afin d'accéder à un document administratif contenant des données à caractère personnel**, **le demandeur doit justifier de la finalité** (légitime, déterminée, etc.) **de l'utilisation (du traitement) des**

[86] Avis n° 167/2022, considérant n° 25.

[87] Voir également les considérants nos 12-14 de l'avis n° 131/2023.

<u>données envisagé</u>, ce qui peut dans certains cas équivaloir à exiger de lui **qu'il justifie d'un intérêt légitime**.

32. Compte-tenu de la grande diversité des documents et informations dont il est question dans le cadre de la publicité passive de l'administration, afin de permettre la conciliation des droits et libertés en présence par l'autorité publique saisie d'une demande, il ne suffit en effet pas d'exiger de la part du demandeur un intérêt exclusivement lorsque l'information concernée « *constitue une appréciation ou un jugement de valeur relatif à* [la] *personne* [concernée] *ou lorsqu'elle se rapporte à un comportement de cette personne dont la divulgation peut manifestement lui causer préjudice* ».

II.2.2. Communication des données par courriel

33. L'article B.I.17, § 4, du Projet prévoit qu'à la suite d'une demande d'accès à un document administratif ou à une information environnementale, « *Le demandeur veille à indiquer la façon dont il souhaite pouvoir prendre connaissance du document ou de l'information environnementale. <u>À défaut de précisions, la communication d'une copie par courriel</u> <u>est privilégiée</u>* » (souligné par l'Autorité).

34. Selon les données concernées, il est possible que ce moyen de communication ne soit cependant pas approprié sur le plan de la sécurité de l'information. L'Autorité a déjà mis en exergue qu'il convenait de **ne pas échanger des données sensibles par courrier électronique,** et elle s'est déjà exprimée quant aux garanties à mettre en place dans ce cadre. Aux considérants nos 25-27 de son avis n°106/2022 du 3 juin 2022 *concernant un projet d'arrêté du Gouvernement wallon modifiant le Code réglementaire wallon de l'action sociale et de la santé en ce qui concerne la promotion de la santé, en ce compris la prévention, en Région wallonne (CO-A-2022-090),* l'Autorité a précisé ce qui suit :

> « *Il incombe au* [responsable du traitement] *de mettre en place des procédures et un canal de communication offrant un niveau de sécurité adapté à la nature des données transmises.*
>
> *En l'occurrence, les données relatives à la santé exigent un haut niveau de confidentialité. Parallèlement aux mesures générales listées dans les normes de la sécurité de l'information (par exemple, NIST CSF, ISO 27001, 27002, 27701, normes minimales de sécurité du réseau de la sécurité sociale), on pourra plus spécifiquement, afin d'atteindre un niveau correct de confidentialité dans la communication par e-mail, mettre en place des mesures concernant tant le canal de transmission que le message (et éventuelles pièces jointes) lui-même, au moyen et à titre d'exemples (non exhaustif) :*

- *De l'utilisation d'une plateforme d'échange en ligne présentant des standards de sécurité conformes à l'état de l'art. Sur internet, l'emploi du protocole TLS dans une version égale ou supérieure à la version 1.2 fait partie des bonnes pratiques ;*

- *D'un logiciel de chiffrement rendant l'information incompréhensible à toute personne ne disposant pas de l'information nécessaire au déchiffrement (la clef), tel l'outil gratuit de compression « 7-zip » où l'on choisira le standard de chiffrement AES-256. On notera la nécessité d'utiliser deux canaux de communication distincts pour l'envoi du message chiffré et de la clef de déchiffrement correspondante (par exemple : courriel puis téléphone) ;*

- *Si l'on veut s'assurer que les informations n'ont pas subi d'altérations lors de la transmission, de l'utilisation d'une technique de hachage. Tout comme pour le chiffrement, on veillera à n'utiliser que des algorithmes reconnus et sûrs (ex., SHA-512 et SHA-3). La fonction de hachage doit être appliquée au texte clair et ajoutée au texte clair avant le chiffrement (pas au texte chiffré).*

Parallèlement à ces mesures, on conseillera également, pour tout système donnant accès à des données sensibles (y compris donc celles relatives à la santé) :

- *Au recours à l'authentification à au moins deux facteurs - l'authentification auprès de la plate-forme par un nom d'utilisateur et un mot de passe n'est pas suffisant*[…]*;*

- *A une politique de mot de passe stricte (un mot de passe aléatoire composé de lettres d'une longueur d'au moins 17 caractères ou un mot de passe aléatoire composé de caractères alphanumériques (a-z, A-Z, 0-9,…) d'au moins 14 caractères) ;*

- *D'exiger des éventuels sous-traitants et sous-sous-traitants le respect des mêmes exigences de sécurité* ».

35. Par conséquent, l'Autorité est d'avis que le Projet doit être adapté afin de ne pas privilégier systématiquement l'envoi des informations concernées par courriel, et de limiter le recours à ce mode de communication aux hypothèses dans lesquelles cela est approprié sur le plan de la sécurité de l'information. Autrement dit, et pour le reste **dans la logique du principe d'*accountability***, selon le traitement de données à caractère personnel en cause, et en particulier selon les données

concernées, **le Projet devrait laisser au responsable du traitement la marge de manœuvre nécessaire pour déterminer *in concreto*, le mode de communication des données**.

II.2.3. Rôle du consentement (informations environnementales)

36. L'article B.I.18, § 3, du Projet, prévoit que, à moins que l'information concernée ne concerne des émissions (auquel cas, les exceptions citées ci-après ne s'appliquent pas), « *L'Autorité publique rejette la demande de consultation, d'explication ou de communication sous forme de copie d'une information environnementale si elle constate que l'intérêt du public servi par la publicité ne l'emporte pas sur la protection de l'un des intérêts suivants* : », notamment : « *5° la confidentialité des données à caractère personnel et des dossiers concernant une personne physique si cette personne n'a pas consenti à la divulgation de ces informations au public, lorsque la confidentialité de ce type d'information est prévue par le droit régional ou européen ; 6° aux intérêts ou la protection de toute personne qui a fourni les informations demandées sur une base volontaire sans y être contrainte par la loi ou sans que la loi puisse l'y contraindre, à moins que cette personne n'ait consenti à la divulgation de ces données* » (souligné par l'Autorité).

37. Le Projet ne définit toutefois pas le fait « *d'avoir consenti* », mais bien le concept de « *consentement* », comme le consentement au sens de l'article 4, 11), du RGPD[88]. L'Autorité ne voit pas d'objection à ce que le Projet permette l'accessibilité d'informations environnementales sous réserve du consentement de la personne concernée au sens du RGPD. Cela étant précisé, **il doit clairement organiser le régime juridique applicable à ce consentement**. L'Autorité a déjà mis en évidence à plusieurs reprises qu'en matière de transparence administrative, la communication de données par l'Autorité concernée consiste en un traitement de données à caractère personnel fondé sur une obligation légale, soit un traitement visé par l'article 6, 1., c), du RGPD. Il appartient à cet égard au demandeur de définir le régime juridique du consentement retenu dans le cadre de son Projet (peut-il être retiré et dans quelles conditions ?). **A défaut de justification particulière qui devrait être avancée par le demandeur, l'Autorité est d'avis que le dispositif du Projet devrait prévoir l'application complète de l'article 7 du RGPD, aux hypothèses visées** par l'article B.I.18, § 3, 5° et 6° du Projet. Dans l'hypothèse où le demandeur prévoirait un régime juridique ne permettant pas le retrait du consentement (à supposer qu'il puisse le justifier au regard du traitement concerné – ce dont doute *a priori* l'Autorité), il lui incomberait alors de mettre également en œuvre, un régime d'opposition permettant à la personne concernée, pour des raisons spécifiques à sa situation, de s'opposer au traitement *a posteriori*[89].

[88] Article A.III.1.84), du Projet.

[89] L'Autorité rappelle que le droit d'opposition dans le cadre du RGPD peut également être exercé *a priori*, c'est-à-dire avant la mise en œuvre du traitement. Cela étant précisé, en l'occurrence, s'agissant d'un traitement de données fondé sur une obligation légale requérant un accord de la part de la personne concernée, cette dernière pourra par conséquent toujours faire obstacle au traitement en ne donnant pas son accord.

II.2.4. Soustraction partielle à la publicité administrative

38. L'article B.I.18, § 5, al. 2, du Projet, prévoit que « *Lorsque, en application des paragraphes* [2, 3 et 4], *un document administratif ou une information environnementale ne doit ou ne peut être soustrait que partiellement à la publicité, la consultation, l'explication ou la communication sous forme de copie est limitée à la partie restante* ».

39. **L'Autorité rappelle sur ce point que des données à caractère personnel n'en sont plus que lorsqu'elles ont fait l'objet d'un traitement d'anonymisation**. A ce sujet, si la suppression de données d'un ensemble de données peut parfois conduire à l'anonymisation des données concernées, tel n'est pas nécessairement toujours le cas (cela dépend des données concernées et des données supprimées : par exemple, il peut ne pas suffire de supprimer l'identité d'une personne concernée pour empêcher son identification/réidentification ou sa singularisation).

II.2.5. Publication de données via internet

40. L'article B.I.4 du Projet reprend une mesure actuelle de publicité active de l'administration consistant notamment à mettre à disposition des informations relatives aux subventions, aux études, aux marchés publics et au personnel (appels à candidats, promotions, etc.).

41. L'Autorité **se réfère avant tout, à titre préliminaire, à ses avis nos 131/2023 et 42/2023** dont les développements valent, *mutatis mutandis*, directement en la matière. A cet égard, le dispositif du Projet doit :

- Expliciter **la finalité** de la mesure de transparence mise en œuvre. Pour rappel, la transparence ne constitue pas en elle-même, une finalité de traitement. Elle répond à un objectif déterminé qui lui, correspond à la finalité du traitement ;

- **Fixer et justifier la durée** pendant laquelle les données à caractère personnel concernée sont mises à disposition via la rubrique transparence des sites internet des autorités publiques ;

- Prévoir un **régime d'opposition spécifique** à disposition de la personne concernée, dès lors qu'il ne peut être exclu en pratique, que pour des raisons spécifiques à sa situation, une personne concernée puisse nécessiter le retrait d'informations la concernant[90]. Cette considération est d'autant plus valable en l'occurrence que des données sont également

[90] L'Autorité rappelle sur ce point que le droit d'opposition peut être mis en œuvre avant et après la réalisation du traitement de données.

publiées concernant les recrutements, remplacements et promotions. Cela étant, ce régime ne peut non plus avoir pour effet de remettre en question l'objectif large de transparence poursuivi par le Projet ;

- L'Autorité attire également l'attention du demandeur sur le fait qu'une fois les données concernées mises à disposition via internet, il sera généralement illusoire de vouloir en maîtriser la circulation ultérieure.

42. Ensuite l'Autorité rappelle le **considérant n° 12 de son avis n° 131/2023**, selon lequel :

> « *La* ***Cour de Justice de l'Union Européenne s'est prononcée à plusieurs reprises dans le domaine de la transparence administrative*****[91]** *et ce qui suit notamment, se dégage de sa jurisprudence. Il appartient à l'auteur de la norme en projet de démontrer que le traitement de données envisagé assure un juste équilibre entre l'objectif poursuivi et les droits et libertés en présence, et ne va pas au-delà de ce qui est nécessaire. Une relation doit exister entre la gravité de l'ingérence et l'objectif d'intérêt général poursuivi. Ainsi,* ***l'objectif poursuivi ne doit pas raisonnablement pouvoir être atteint de manière aussi efficace par d'autres moyens moins attentatoires*** *aux droits fondamentaux des personnes concernée, les limitations à la protection des données devant être limitée au strict nécessaire. En particulier s'agissant de la publication de données via internet,* ***il importe que le législateur mène une analyse au terme de laquelle la publication via internet sans aucune restriction d'accès est strictement nécessaires aux objectifs poursuivis,*** *plutôt que par exemple, une accessibilité plus limitée de ces données, à des personnes s'identifiant voire le cas échéant, qui justifieraient en outre d'un intérêt légitime à y accéder*[92] » (numérotation des notes de bas de page modifiée par l'Autorité dans le présent avis) ».

43. L'article B.1.4, § 1er, al. 1er, 5°, du Projet prévoit que les données suivantes sont publiées via les rubriques transparence des sites internet de chaque autorité publique :

---

91 « *Voir notamment : CJUE (Gr. Ch.), arrêt du 29 juin 2010, Commission c/ The Bavarian Lager, aff. C-28/08 ; CJUE (Gr. Ch.), arrêt du 22 novembre 2022, WM, Sovim SA c. Luxembourg Business Registers, affs C-37/20 et C-601/20 (informations relatives aux bénéficiaires effectifs d'entités telles que les sociétés) ; CUJE (Gr. Ch.), arrêt du 9 novembre 2010, Scheke, Eifert c/ Land Hessen, affs C-92/09 et C-93/09 (informations relatives au subsides et fonds dans le domaine agricole) ; CUJE (Gr. Ch.), arrêt du 5 avril 2022, G.D. c/ Commisioner of An Garda Siochana et al., aff. C-140/20 ; CUJE (Gr. Ch.), 1er août 2022, OT c/ Vyriausioji tarnybines etikos komisija, aff. C-184/20 (informations relatives aux déclarations d'intérêts) ; CJUE (Gr. Ch.), arrêt du 22 juin 2021, B-Points de pénalité, aff. C-439/19 (informations relatives à des infractions en matière de circulation routière)* ».

92 « *Voir les articles 4 et 6, de la loi du 11 avril 1994 relative à la publicité de l'administration. Sur l'éventuelle nécessité de devoir justifier d'un intérêt légitime, la nécessité de la mise à disposition de données à caractère personnel, voir par exemple CJUE (Gr. Ch.), arrêt du 29 juin 2010, Commission c/ The Bavarian Lager, aff. C-28/08 ; CJUE (Gr. Ch.), arrêt du 22 novembre 2022, WM, Sovim SA c. Luxembourg Business Registers, affs C-37/20 et C-601/20, considérants nos 68-74 et 85 ; CJUE (Gr. Ch.), arrêt du 22 juin 2021, B-Points de pénalité, aff. C-439/1, considérants nos 119-122* ».

> « *les appels à candidats et les conditions de recrutement, de promotion ou de remplacement de tous les emplois qu'elles entendent pourvoir, publiés dans les sept jours ouvrables de la décision de procéder à un recrutement, une promotion ou un remplacement, ainsi que les décisions de recrutement, de promotion ou de remplacement des emplois des agents de niveau A qu'elles pourvoient, publiées dans les sept jours ouvrables de la décision* » (souligné par l'Autorité).

44. L'exposé des motifs des décret et ordonnance conjoints de la Région de Bruxelles-Capitale, la Commission communautaire commune et la Commission communautaire française du 16 mai 2019 relatifs à la publicité de l'administration dans les institutions bruxelloises précisent ce qui suit à propos de cette disposition :

> « *S'agissant des décisions de recrutement, de promotion ou de remplacement en elles-mêmes, il est tenu compte de ce que, dans son avis 59/2018 du 4 juillet 2018, l'Autorité de protection des données suggère de limiter la publication sur le site internet des autorités aux décisions de recrutement/promotion/remplacement qui sont elles-mêmes publiées au Moniteur belge*[93]*. La doctrine rappelle à cet égard qu'« il est d'usage que les arrêtés de nomination d'agents du niveau 1 soient publiés au Moniteur belge » (Jean SAROT et al., Précis de fonction publique, Bruylant, Bruxelles, 1994, p. 194)* »[94] (souligné par l'Autorité).

45. L'Autorité est d'avis que **cette justification du traitement prévu par la disposition en projet est insuffisante**. Il incombe tout d'abord au demandeur d'identifier en vertu de quelles règles et à quelle(s) finalité(s) les décisions de recrutement, promotion et de remplacement concernées sont publiées au Moniteur Belge. Ce qui permettra, le cas échéant, de justifier la différence de traitement entre personnes concernées selon leur niveau de fonction, dans le cadre de la publication initiale des données au Moniteur Belge. Dans un deuxième temps ensuite, le Projet doit justifier la raison pour laquelle une publication complémentaire via les rubriques transparence des sites internet des autorités publiques est nécessaire compte-tenu de la finalité poursuivie par le Projet lui-même.

II.4. PARTAGE ADMINISTRATIF DE DONNÉES (ÉCHANGES DE DONNÉES ENTRE AUTORITÉS PUBLIQUES) (LIVRE C.IV., TITRE 2)

[93] Au considérant n° 13 de son avis n° 59/2018 du 4 juillet 2018 *concernant un projet de décret et ordonnance conjoints relatifs à la publicité de l'administration dans les institutions bruxelloises (CO-A-2018-038)*, l'Autorité a en effet précisé ce qui suit :

« *A l'article 17 du projet, mention est faite, parmi les informations communicables, celles relatives aux décisions de recrutement, de promotion ou de remplacement. Cela apparaît comme excessif au regard du principe de proportionnalité dès lors que la règle ainsi édictée viserait également les agents administratifs dont la nomination n'est pas appelée à être publiée au Moniteur belge. L'APD invite donc le demandeur à limiter cette disposition aux seules personnes nommées par cette voie, que celles-ci exercent ou non un mandat public* ».

[94] Parlement Bruxellois, session ordinaire 2018-2019, 4 avril 2019, doc. n° A-862/1, n° B-172/1, p. 8.

II.4.1. Partage administratif en général

46. L'article C.IV.4 du Projet, intitulé « *Partage administratif par défaut et demande de partage administratif* », dispose que :

> « *Les Autorités Publiques organisent des partages administratifs de données entre elles, gratuitement, sauf si ces partages administratifs sont contraires à une règle de droit ou s'ils portent atteinte aux droits des tiers sur les données soumises au partage administratif.*
>
> *Les modalités des demandes de partage administratif formulées par les Autorités publiques destinataires sont déterminées par le Bureau de la donnée en concertation avec le Comité de Gouvernance de la donnée.*
>
> *L'absence de réponse à une demande de partage administratif est assimilée à un refus de partage administratif dans le chef de l'Autorité publique productrice des données* » (souligné par l'Autorité).

47. L'article C.II.3, § 1er, du Projet s'inscrit dans la même logique en prévoyant que « *Par défaut, les Autorités publiques organisent le partage administratif* [95] *de données entre elles afin d'améliorer l'exercice de leurs missions de services publics et de leurs obligations d'intérêt général* [96]*, et, d'alléger le cas échéant la charge administrative des citoyens* [97] » (souligné par l'Autorité)[98].

48. L'Autorité est d'avis que sur le plan des principes, **ces dispositions renversent le paradigme juridique actuellement applicable aux traitements de données à caractère personnel en droit belge, conformément aux principes de légalité et de prévisibilité** consacrés dans les articles 8 CEDH et 22 de la Constitution. Ce faisant, **le Projet transpose la logique du traitement de données issues de sources authentiques de données à tout échange de données auquel est partie une autorité publique bruxelloise**[99], à charge pour celles-ci de conclure un protocole d'accord à cette fin[100]. Alors qu'en principe et en toutes hypothèses, un traitement de données à

---

[95] Voir la note de bas de page n° 12 pour la définition du concept de partage administratif.

[96] L'Autorité relève au passage qu'il ne s'agit pas d'une finalité déterminée.

[97] L'Autorité relève au passage qu'il ne s'agit pas d'une finalité déterminée.

[98] L'exposé des motifs s'énonce comme suit à ce sujet :

« *Les Autorités publiques sont appelées à organiser des partages administratifs entres elles conformément aux dispositions du présent titre, pour les raisons reprises dans l'exposé des motifs, à savoir alléger la charge administrative des citoyens, créer des synergies, améliorer la qualité des services publics et d'intérêt général, mutualiser certains frais de fonctionnement etc.* ».

[99] L'Autorité s'interroge d'ailleurs, avec la mise en place d'un tel principe, sur l'utilité qu'il y aurait ensuite, de mettre en œuvre des sources authentiques bruxelloises. L'Autorité note d'ailleurs en passant, qu'à sa connaissance, il n'existe pas en droit positif bruxellois de source authentique de données au sens de l'ordonnance du 8 mai 2014 *portant création et organisation d'un intégrateur de services régional*.

[100] Voir l'article C.IV.8 du Projet.

caractère personnel ne peut avoir lieu **que lorsqu'il est fondé juridiquement dans le cadre d'une compétence ou d'une obligation attribuée à une autorité publique** (presque toujours dans le cadre des traitements de données réalisés par les Autorités publiques, le traitement de données a lieu dans les cas visés à l'article 6, 1., c) et d)) et que ses **éléments essentiels sont déterminés par une norme du rang de loi**. Étant entendu que selon les traitements de données concernés, l'encadrement par une norme du rang de loi sera **plus ou moins étendu**[101]. Autrement dit, il ne suffit pas pour qu'un traitement de données soit réalisable, qu'aucune disposition particulière ne s'y oppose.

49. Afin d'être complet, l'Autorité rappelle également qu'en tout état de cause un **protocole d'accord ne suffit jamais à fonder juridiquement un échange de données entre autorités publiques**[102].

[101] La pratique d'avis du Centre de Connaissances de l'Autorité illustre de manière abondante les manières de mettre en œuvre ses principes (voir également de manière générale, l'avis standard n° 65/2023 du 24 mars 2023 *relatif à la rédaction des texte normatifs*).

[102] L'Autorité a réitéré cette position et se réfère ici à sa recommandation n° 02/2020 du 31 janvier 2020 *relative à la portée de l'obligation de conclure un protocole afin de formaliser les communications de données à caractère personnel en provenance du secteur public fédéral,* pp. 9-10 :

« *Aux termes de l'article 20 de la LTD,* ***l'obligation de conclure un protocole*** *n'existe que lorsque la communication de données à caractère personnel en provenance d'une autorité publique fédérale* ***est nécessaire au respect d'une obligation légale*** *à laquelle le responsable du traitement est soumis, ou lorsqu'elle est* ***nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement****, étant entendu que l'obligation légale ou la mission d'intérêt public qui légitime la communication de données à caractère personnel peut exister tant dans le chef du responsable du traitement qui communique les données à caractère personnel que dans le chef du responsable du traitement qui réceptionne ces données.*

Cette exigence doit se comprendre à la lumière du principe de l'attribution des compétences administratives, du principe de spécialité des personnes morales ainsi que du principe de légalité qui préside à la définition des conditions auxquelles l'administration peut interférer avec le droit à la protection de la vie privée, lequel inclut le droit à la protection des données à caractère personnel[…]. Aux termes du principe de l'attribution des compétences administratives, qui est consacré par l'article 105 de la Constitution et 78 de la loi spéciale du 8 août 1980 de réformes institutionnelles, les autorités administratives n'ont d'autres pouvoirs que ceux que leur attribuent formellement la Constitution et les lois et décrets portés en vertu de celle-ci. En outre, le principe de spécialité des personnes morales dispose que toute institution dotée de la personnalité juridique ne peut agir que pour atteindre le(s) but(s) pour le(s)quel(s) elle a été créée, étant entendu que seule une norme législative peut confier une mission de service public à une personne morale. En outre, comme le Conseil d'Etat l'a rappelé dans son avis sur l'avant-projet de loi "relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel", « un transfert de données d'une autorité publique à une autre constitue une ingérence dans le droit à la protection de la vie privée des personnes concernées. En vertu de l'article 8 de la Convention européenne des droits de l'homme et de l'article 22 de la Constitution, tel qu'interprété par une jurisprudence constante de la Cour constitutionnelle, pareille ingérence doit notamment reposer sur une base légale, être proportionnée par rapport à l'objectif poursuivi et être organisée de manière suffisamment précise pour être prévisible pour le citoyen »[…]. ***Ainsi, une autorité publique ne peut traiter – et donc communiquer – des données à caractère personnel que si cette communication est nécessaire au respect d'une obligation imposée par ou en vertu d'une norme législative à l'un des responsables du traitement ou si elle est nécessaire à l'exécution d'une mission d'intérêt public qui a été dévolues à l'un des responsables du traitement par ou en vertu d'une norme législative****. Comme l'a souligné la CPVP dans son avis concernant l'avant-projet de loi "relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel", les communications de données à caractère personnel en provenance du secteur public doivent reposer sur une base légale, étant entendu qu'« un protocole d'échange ne pourra jamais constituer la base légale d'un traitement de données »[…].*

*Cette exigence constitutionnelle implique que, dans l'immense majorité des cas, les communications de données à caractère personnel par des autorités publiques sont « nécessaire[s] au respect d'une obligation légale à laquelle le responsable du traitement est soumis » (****A****) ou « nécessaire[s] à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » (****B****). Toutefois, on ne peut pas exclure que, dans certaines circonstances, très rares, une communication de données à caractère personnel en provenance du secteur public puisse reposer sur un autre fondement juridique prévus par l'article 6 du RGPD. Aux termes de l'article 20 de la LTD, de telles communications ne doivent pas être formalisées par un protocole (****C****)* » (références omises par l'Autorité dans le présent avis).

50. Indépendamment de ces préoccupations de nature juridique du droit de la protection des données, l'exposé des motifs **n'explique pas non plus concrètement pour quelle raison un tel changement d'approche serait nécessaire**[103].

II.4.2. Sources authentiques de données

51. L'article C.II.3, § 2, al. 1er, du Projet, dispose que « *Les Autorités publiques utilisent les sources authentiques afin de collecter les données dont elles ont besoin* » (souligné par l'Autorité).

52. Conformément aux principes de proportionnalité et au principe de minimisation des données consacré dans l'article 5, 1., c), du RPGD, les autorités publiques ne traitent que les données qui sont **nécessaires à l'exécution des missions d'intérêt public ou des obligations légales qui leur incombent**. Le Projet doit par conséquent être adapté en ce sens, d'autant plus qu'il présente un certain flou en ce qu'il exige la valorisation des données.

53. L'article C.IV.12 du Projet, intitulé « *Partage administratif de données issues de sources authentiques aux fins de collecte unique* » (souligné par l'Autorité), dispose en son paragraphe 1er que :

> « *Les partages administratifs de données issues de sources authentiques visent la mise à disposition de ces données au profit des Autorités publiques destinataires afin qu'elles n'en organisent plus elle-même la collecte* » (souligné par l'Autorité).

---

[103] Au sujet de l'article C.II.3 du Projet, l'exposé des motifs énonce ce qui suit :

« *Le paragraphe 1er énonce le principe du partage par défaut, entre les Autorités publiques, des données qui peuvent l'être. Ce principe de partage est l'objectif général du mécanisme de partage administratif au sens du Code, lequel reçoit une définition et des modalités organisationnelles particulières au travers du livre C.IV.*

Ce principe vise à encourager les institutions à échanger dans l'objectif de diminuer la charge administrative des citoyens bruxellois.

Un tel principe est nécessaire à l'amélioration de l'efficacité des missions confiées aux Autorités publiques ainsi qu'à la simplification de la vie des citoyens.

Le paragraphe 2 énonce le principe de la collecte unique de données, ou principe dit « once only ».

La consécration de données issues de sources authentiques, comme organisée par le Code, permet d'organiser le partage de ces données entre Autorités publiques de manière à ce que le citoyen n'ait plus à redonner les données qu'il a déjà fournies à d'autres Autorités publiques. Il s'agit d'organiser une collecte unique des données – principe du once only – au départ de données dont la qualité est garantie du fait du cadre légal qui leurs est applicable et décrit dans le livre C.IV.

Enfin, le paragraphe 3 instaure également le principe du partage des données publiques vers l'extérieur dans le cadre de réutilisations » (souligné par l'Autorité).

Plus loin, l'exposé des motifs en rappelant « *l'importance d'un partage rendu plus efficace entre les Autorités publiques* », précise qu' « *un certain nombre d'études commandées par l'Agence fédérale pour la simplification administrative montrent très clairement que le partage de données disponibles peut entraîner une diminution significative des charges administratives* [(référence étant faite à la « Note au gouvernement de la Région de Bruxelles-Capitale sur une stratégie bruxelloise sur les données »)], et que « *l'application du principe de la collecte unique de données a également un effet positif sur le fonctionnement et l'efficience des autorités publiques*[…] *dans le cadre de l'exécution de leurs missions* ».

L'exposé des motifs exprime encore ce qui suit :

« *L'idée générale poursuivie par le présent livre est que les flux de données ne peuvent avoir lieu que conformément au principe de légalité. Le livre C.IV constitue la base légale des flux qu'il régit, sans préjudice, le cas échéant, de l'adoption de règles particulières et spécifiques à chaque flux* » (souligné par l'Autorité). Analyse qui ne peut être suivie pour les raisons développées dans le corps du présent avis.

54. L'Autorité insiste tout d'abord sur le fait que **le recours aux sources authentiques de données ne se justifie pas qu'à la seule fin d'éviter aux autorités publiques d'organiser elles-mêmes la collecte des données auprès des personnes concernées**[104]. La **qualité de la donnée** traitée[105] constitue également un élément déterminant dans la justification du recours aux sources authentiques de données, et un élément central dans l'identification de telles sources de données[106]. *En outre, l'établissement d'une source authentique de données* ***nécessitera qu'une attention particulière de la part du législateur et du responsable du traitement soit réservée à la sécurisation de la communication des données****, dès lors qu'une telle source a pour vocation d'être réutilisée et partant, de donner lieu à de fréquentes communications de données*

55. Par ailleurs, l'Autorité rappelle que la consécration dans une norme du rang de loi (en l'occurrence, une ordonnance) du principe de collecte unique des données (principe « *only once* ») **ne dispense pas le législateur et les autorités publiques de veiller à l'application de l'article 6, 4., du RGPD** : la collecte indirecte d'une donnée demeure un traitement ultérieur de données soumis à l'article 6, 4., du RGPD[107].

56. L'article C.IV.13 du Projet concerne les « ***clefs d'identification*** » qui doivent être utilisées. Son paragraphe 1er prévoit que dans le cadre de la mise à disposition des données issues de sources

---

[104] Il est à souligner sur ce point que la disposition ne vise pas explicitement la collecte des données *auprès de la personne concernée*. Ce qui devrait être le cas.

[105] Exactitude et caractère à jour, conformément à l'article 5, 1., d), du RGPD.

[106] Voir encore récemment à ce sujet, l'avis n° 143/2023, considérant n° 39.

[107] Ainsi en ce sens, selon le Contrôleur Européen de la Protection des Données :

« *Le RGPD introduit une nouveauté: l'article 6, paragraphe 4, codifie également une exception au principe de limitation de la finalité lorsque le traitement ultérieur repose sur le consentement ou sur le droit de l'Union ou d'un État membre[…].*

Il ne s'agit toutefois pas d'une autorisation illimitée d'adopter tout texte législatif général et large permettant de réutiliser sans fin des données à caractère personnel entre différents ministères. Conformément à la Charte des droits fondamentaux, la loi doit respecter certaines exigences pour qu'il puisse être dérogé au principe de limitation de la finalité.

En particulier, elle doit constituer «une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, paragraphe 1». Ces objectifs couvrent la sécurité nationale, la défense, la lutte contre la criminalité et d'autres objectifs spécifiquement mentionnés d'intérêt public.

Certains de ces objectifs d'intérêt public peuvent être pertinents pour certaines applications spécifiques et ciblées du principe «une fois pour toutes» (par exemple, certaines mesures nécessaires et proportionnées pour lutter contre la criminalité au titre de l'article 23, paragraphe 1, point d) ou en lien avec la perception des impôts en vertu du point e) de la même disposition).

L'allégement de la charge administrative sur les personnes physiques ou les organisations, l'efficacité accrue des procédures administratives et l'économie de temps et de ressources, qui sont souvent les objectifs premiers des applications du principe «une fois pour toutes» constituent sans nul doute des objectifs d'intérêt public valables. Néanmoins, ils ne sont pas spécifiquement mentionnés dans la liste visée à l'article 23, paragraphe 1, et ne constituent pas en soi un motif licite permettant de restreindre la portée du principe de limitation de la finalité pour atteindre ces objectifs. Cela étant, comme indiqué plus haut, on ne peut exclure que dans certains cas spécifiques, l'un ou l'autre des fondements juridiques des limitations visées à l'article 23, paragraphe 1, point d), puisse être approprié.

En conclusion, conformément aux observations qui précèdent et à moins qu'un motif approprié de limitation visé à l'article 23, paragraphe 1, soit disponible ou que les personnes concernées aient donné leur consentement, le principe de limitation de la finalité doit être respecté, même lorsqu'une législation de l'Union ou d'un État membre prévoit l'application du principe «une fois pour toutes » (souligné et référence omise par l'Autorité), CEPD, Avis n° 8/2017 *sur la proposition de règlement établissant un portail numérique unique et sur le principe 'une fois pour toutes'*, pp. 11-12.

authentiques, pour l'identification de personnes physiques, les autorités publiques utilisent notamment le numéro de Registre National[108]. Le paragraphe 3 prévoit quant à lui ce qui suit :

> « *Dans le cadre de l'accomplissement d'une obligation légale d'information, les personnes physiques et morales utilisent :*
>
> *1° le numéro du Registre national attribué en exécution de l'article 2, alinéa 2, de la loi du 8 août 1983 organisant un Registre national des personnes physiques, ou*
>
> *2° le numéro d'identification de la Banque attribué en exécution de l'article 4, § 2, alinéa 3, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité sociale et le numéro d'entreprise attribué Fen exécution de l'article III.17 du Code de droit économique* » (souligné par l'Autorité).

57. L'Autorité ne comprend par la portée de cette disposition au sujet de laquelle l'exposé des motifs ne précise rien. Autrement dit, **cette disposition doit être omise ou clarifiée. L'Autorité réserve son analyse à son sujet**.

58. En ce qui concerne la **désignation des sources authentiques de données,** l'article C.IV.15, § 1er [109], du Projet prévoit que :

> « *Sans préjudice des sources authentiques reconnues par des Autorités publiques tierces, le Gouvernement, le Collège réuni et le Collège, désignent par arrêté, les sources authentiques dont l'Autorité publique désignée comme producteur de la source authentique relève de leur compétence.*
>
> *Par dérogation à l'alinéa 1er, les sources authentiques comprenant des données à caractère personnel sont désignées par décret ou ordonnance selon la Collectivité publique dont dépend l'Autorité publique désignée producteur de la source authentique* » (souligné par l'Autorité).

59. L'Autorité rappelle que conformément aux principes de prévisibilité et de légalité évoqués précédemment et consacrés dans des normes hiérarchiquement supérieures à l'ordonnance (soit la Constitution et la CEDH), il ne suffit pas que la source authentique de données soit désignée par une norme du rang de loi (en l'occurrence, un décret ou une ordonnance) : l'ensemble des éléments

[108] L'exposé des motifs relève ce qui suit : « *Cette obligation vient en réalité palier le fait qu'aujourd'hui certaines Autorités publiques bruxelloises n'ont pas encore demandé les autorisations nécessaires pour disposer de ces numéros. L'absence d'autorisation ne pourra donc plus servir d'excuses pour l'absence de partages administratifs des données disponibles dans la source authentique concernée* ». Sur la motivation du recours au numéro du Registre National, voir plutôt les considérants nos 31-33 de l'avis n° 143/2023.

[109] Le paragraphe indiqué comme « § 3 » dans le Projet est en réalité l'alinéa 1er du paragraphe 1er de l'article C.IV.15.

essentiels des traitements de données liés à cette source authentique doivent être consacrés dans une norme du rang de loi.

60. Elle rappelle encore que l'article 4, 1), du RGPD définit la donnée à caractère personnel comme « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou social* » (souligné par l'Autorité). Il est ainsi clair que pour qu'une source authentique « ***comprenne*** » des données à caractère personnel, il n'est pas nécessaire que la personne concernée y soit directement identifiée (nominativement ou via son numéro de Registre National). Ce commentaire est important à l'égard d'un système d'information tel qu'UrbIS dans lequel des informations peuvent être liées à des adresses, des numéros de parcelles cadastrales[110]. **L'élément décisif quant à l'application des principes de transparence et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution est que la source authentique de données soient sollicitées dans le cadre d'un traitement de données à caractère personnel.**

61. En outre, **l'Autorité souligne que la définition de « *source authentique bruxelloise* » doit être adaptée de manière à être mise en conformité à l'article C.IV.15, § 1er du Projet** : si la source authentique bruxelloise « *comprend* » des données à caractère personnel, celle-ci doit être désignée par décret ou ordonnance.

62. Dans cette logique, l'article C.IV.15, § 4, du Projet prévoit ce qui suit :

> « *L'acte de désignation visé au paragraphe 1er indique, notamment, pour chaque source authentique :*
>
> *1° l'identité de l'Autorité publique producteur de la source authentique, chargé de la collecte des données, de leur mise à jour, de leur mise à disposition et de tout autre traitement pertinent et nécessaire à son maintien, en fonction de l'état de l'art et de l'évolution des technologies ;*
> *2° les modalités selon lesquelles sont tenues à jour et rendues accessibles les données dont l'hébergement est confié à l'Autorité publique producteur de la source authentique ;*

[110] Voir le considérant n° 16, avant-dernier tiret.

3° la ou les finalités poursuivies par l'Autorité publique producteur par la constitution de la source authentique lors la collecte des données visées ;

4° la liste des données contenues dans la source authentique ;

5° les modalités particulières de financement de la collecte des données comprises dans la source authentique, de leur mise à jour, de leur mise à disposition et de tout autre traitement pertinent et nécessaire à son maintien.

Pour ce qui concerne la désignation de sources authentiques comprenant des données à caractère personnel, le décret ou l'ordonnance indique également:

- *les éléments essentiels du traitement;*
- *les mesures prévues protégeant les droits des personnes concernées;*
- *les obligations de transparence prévues à l'intention des personnes concernées* » (souligné par l'Autorité).

63. L'Autorité rappelle que ces **dispositions sont en tout état de cause sans préjudice des normes hiérarchiquement supérieures qu'elles rappellent** du moins pour partie, à savoir les normes découlant de l'application de l'article 8 CEDH, 22 de la Constitution et du RGPD lui-même, d'application directe. Ainsi, ce sont le cas échéant de mesures de protection et d'obligation de transparence **spécifiques** dont il sera question dans les actes de désignation, dès lors que l'ensemble des obligations du RGPD sont d'application directe et ne peuvent pas être retranscrits en droit national[111]. **L'Autorité est d'avis que l'exposé des motifs doit souligner ce point de hiérarchie des normes**, **qui devra l'être à nouveau dans l'exposé des motifs des actes de désignation (décret ou ordonnance) des sources authentiques impliquant le traitement de données à caractère personnel**.

64. Par ailleurs, l'Autorité est d'avis que **le Projet devrait déterminer les critères sur la base desquels une banque de données peut être désignée comme une source authentique de données**, en réservant une attention particulière quant à la qualité de la donnée (exactitude, caractère à jour, etc.) concernée et sa relation avec la mission d'intérêt public dont est chargé le responsable du traitement de la source authentique[112]. Le Projet comporte à cette fin des concepts utiles au titre du principe de qualité des données consacré dans l'article C.II.5, selon lequel la « *qualité de données se*

[111] L'Autorité rappelle que l'applicabilité directe des règlements européens emporte l'interdiction de leur retranscription dans le droit interne en raison du fait qu'un tel procédé pourra créer « *une équivoque en ce qui concerne tant la nature juridique des dispositions applicables que le moment de leur entrée en vigueur* » (CJUE, arrêt du 7 février 1973, *Commission c/ Italie*, aff. C-39/72, considérant n° 17 ; voir également CJUE, arrêt du 10 octobre 1973, *Fratelli Variola S.p.A. c/ Administration des finances italienne*, aff. C-34/73, considérant n° 11 ; CJUE, arrêt du 31 janvier 1978, *Ratelli Zerbone Snc c/ Amministrazione delle finanze dello Stato*, aff. C-94/77, considérants nos 24-26).

[112] Voir notamment à ce sujet, les considérants nos 38-39 l'avis n° 143/2023.

définit sous différentes dimensions complémentaires, à savoir notamment : 1° Consistance, 2° Exactitude, 3° Exhaustivité, 4° Vérifiabilité, 5° Validité, 6° Unicité, 7° Intégrité, 8° Ponctualité ».

II.4.3. Base de données issues de sources authentiques

65. L'article C.IV.16 du Projet prévoit la possibilité de désigner des bases de données constituées au départ de données issues de sources authentiques, comme bases de données issues de sources authentiques. Plus précisément, il est formulé comme suit :

> « *Des bases de données constituées au départ de données issues de sources authentiques sont désignées en tant que base de données issues de sources authentiques par décret ou ordonnance selon la collectivité publique dont dépend l'Autorité publique désignée producteur de la base de données issues de sources authentiques.*
> *L'article C. IV. 15, §2 à 4 s'applique à la procédure de désignation des bases de données issues de sources authentiques mutatis mutandis.*
> *Dans le cadre de l'application du Code, les bases de données issues des sources authentiques et les données qui en sont issues, sont assimilées respectivement à des sources authentiques et leurs données, à des données issues de sources authentiques* ».

66. L'exposé des motifs, qui **ne justifie pas de la nécessité de recourir à la mise en œuvre de telles bases de données**, précise que « *Cette procédure législative vise donc* ***la désignation de super bases de données*** *revêtues d'une valeur identique à celles des sources authentiques qui la composent exclusivement* » (souligné et mis en gras par l'Autorité).

67. L'Autorité est d'avis que cette approche est doublement problématique.

68. Premièrement, au **considérant n° 13 de son avis n° 65/2019** du 27 février 2019 *concernant 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 s'est interrogée au sujet du concept (équivalent) de banque de données issues de sources authentiques : « *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*[113]. ***Pour une protection accrue de la vie privée des personnes concernées, la même Commission s'est également clairement positionnée en faveur de***

[113] « *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* ».

l'intégration de services plutôt que de l'intégration de données[114]. *Autrement dit,* ***pour ces raisons, le recours aux banques de données issues de sources authentiques devrait être exclu*** » (numérotation des références modifiée dans le présent avis et gras et souligné ajoutés dans le présent avis). Bien que le concept de base de données issues de sources authentiques de données existe en droit positif bruxellois (sans pour autant, à ce jour, qu'à la connaissance de l'Autorité, une telle banque de données existe[115]), **ces considérations valent de la même manière dans le présent avis**.

69. Le concept de banques de données issues de sources authentiques **est en effet contraire au principe et à la définition (la finalité) même des sources authentique de données**. C'est ainsi à juste titre que le dispositif du Projet, dans son article A.III.1.31), définit la source authentique comme « *toute base de données comprenant des données qui font foi comme données uniques et originales concernant la personne ou le fait concerné(e) dont la gestion est assurée exclusivement par une Autorité publique ou une Autorité publique tierce, désigné comme producteur de la base de donnée, et dont le contenu est destiné à faire l'objet de partages administratifs obligatoires conformément au principe de la collecte unique* » (souligné par l'Autorité)[116]. Le concept de base de données issues de sources authentiques est problématique à plusieurs égards :

- Il **rompt avec la logique juste exposée** dès lors qu'une donnée authentique serait désormais accessible dans deux sources différentes qui de surcroît sont toutes deux présentées comme authentiques (de même valeur) et ce **alors que par définition, le responsable du traitement de la banque de données issues de sources authentiques aura une moins bonne relation avec la donnée concernée** (finalité de sa collecte originale, relation entre la mission de service public et la donnée concernée et par conséquent expertise et expérience en lien avec la donnée, relation le cas échéant avec la personne concernée, etc.), ce qui est contraire à la finalité du recours aux sources authentiques ;

- Outre ce problème de principe directement lié à la qualité des données, l'intégration de données authentiques provenant de différentes sources dans une même banque de données augmente pour d'autres raisons encore, les risques pour les droits et libertés des personnes concernées. Ainsi, et comme l'avais mis en exergue la Commission pour la Protection de la

[114] « *Recommandation de la Commission de la Protection de la Vie Privée n° 03/2009* [du 1er juillet2009 *d'initiative concernant les intégrateurs dans le secteur public*], *points nos 5-12* ».

[115] Voir ultérieurement, les développements relatifs à UrbIS.

[116] L'exposé des motifs du Projet rappelle encore que « *Comme les données issues de sources authentiques ne seront gérées que par un seul service public, elles ont une valeur unique et originale dans l'ensemble de l'écosystème bruxellois* » ; « *Une source authentique est une base de données particulière à laquelle est attribuée une valeur particulière du fait que cette base de données n'est gérée que par une seule Autorité publique, qualifiée de producteur au sens du présent Code* ». Le dispositif du Projet ne consacre d'ailleurs pas de définition propre pour le concept de base de données constituées au départ de sources authentiques de données.

Vie Privée évoquée plus haut, permettre l'intégration de données (en l'occurrence, de surcroît, authentiques), **implique de permettre la multiplication des copies de données qui circulent, ce qui entraîne un problème de mise à jour des données**. Mais encore, l'Autorité relève que cette approche peut aussi poser question au regard du principe de minimisation des données ;

- La Commission pour la Protection de la Vie Privée l'avait encore mis en évidence, la concentration des données (en l'occurrence, de surcroît, authentiques) dans un même système d'information **augmente les risques pour la sécurité de l'information** ;

- Enfin, le recours à une banque de données issues de sources authentiques présente un **risque significatif de détournement de finalité et une perte de contrôle de la source authentique de données sur le traitement des données qu'elle a vocation à communiquer**. Il convient de rappeler que le responsable du traitement de la source authentique de données est responsable de la communication des données aux autorités publiques qui entendent traiter les données y accessibles. Notamment, techniquement et administrativement, cette instance perd le contrôle de l'échange de la données (notamment, vérification du destinataire, de la finalité et des données nécessaires) une fois que celle-ci est disponible ailleurs, via une autre banque de données. S'ensuit donc encore en pratique une dilution des responsabilités et une multiplication des intervenants pour la personne concernée. Et **ces risques sont d'autant plus importants lorsque la source authentique et la banque de données issues de sources authentiques relèvent de différents niveaux de pouvoir**. Or c'est également bien dans le sens de la consultation de sources authentiques d'autres niveaux de pouvoir que s'inscrit le Projet.

70. Deuxièmement sur ce point précisément, il se dégage explicitement des définitions consacrées dans le Projet que les bases de données issues de sources authentiques pourraient contenir des **données issues de sources authentiques relevant d'un autre niveau de pouvoir** (Etat fédéral par exemple). Or à ce sujet, l'Autorité réitère le **considérant n° 14 de son avis n° 65/2019** juste cité : « *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*[117]*. 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*** » (gras ajouté par l'Autorité dans le présent avis). Pour le reste, s'il appartient

[117] En l'occurrence conclu entre la Région wallonne et la Communauté française.

au Conseil d'Etat de fixer le demandeur quant à la question de la répartition des compétences, l'Autorité ne perçoit pas pour quel motif, au titre des pouvoirs implicites, une entité fédérée devrait être compétente pour dupliquer les données authentiques d'un autre niveau de pouvoir (auxquelles par définition, elle a accès[118]).

71. **En conclusion** sur ce point, l'Autorité est d'avis que **le concept de base de données issues de sources authentiques de données doit être abandonné.**

72. Au passage, dans un sens similaire aux considérations précédentes relatives à la répartition des compétences, s'agissant de la nécessité de recourir à l'intégrateur de service bruxellois, l'Autorité se réfère au considérant n° 43 de son **avis n° 143/2023**, selon lequel notamment : « […] *Sur ce dernier point en effet, compte-tenu des règles répartitrices de compétences (au sujet desquels il appartiendra in fine au Conseil d'Etat et à la Cour constitutionnelle de se prononcer), l'Autorité est d'avis que* ***le Projet doit être sans préjudice des règles régissant les sources authentiques relevant d'une autre entité fédérale ou fédérée et ne peut notamment imposer des obligations spécifiques aux responsables du traitement de celles-ci*****[…]** » (référence omise par l'Autorité dans le présent avis).

II.5. RÉUTILISATION DES DOCUMENTS ET DES DONNÉES PUBLIQUES (LIVRE C.IV, TITRE 3)

II.5.1. Portée des deux régimes de réutilisation

73. Le Titre 3 du Livre C.IV. est dédié à la réutilisation des documents et des données publiques[119] et consacre, conformément à l'article C.IV.17 du Projet, **deux régimes de réutilisation** : un premier régime, applicable aux documents ouverts accessibles librement et aux documents partageables conformément à la transposition de la Directive Réutilisation ; un second concernant les données protégées, visé par le Règlement sur la Gouvernance des Données.

74. De manière plus générale, l'article C.II.3, § 3, du Projet prévoit que « *Les Autorités publique garantissent également par défaut la réutilisation de leurs données publiques* [120] *par des opérateurs privés* » (souligné par l'Autorité). L'article C.II.4, § 2, du Projet, prévoit que « *Les Autorités publiques organisent la réutilisation de leurs données conformément au titre 3 du livre C. IV. Les Autorités publiques mettent à disposition leurs données ouvertes* [121]*, en assurant le plus haut degré*

[118] A défaut, elle ne pourrait pas les dupliquer.

[119] Voir la note de bas de page n° 4

[120] Voir la note de bas de page n° 4.

[121] Voir la note de bas de page n° 5.

d'ouverture. *A défaut, si cela s'avère impossible, les Autorités publiques adoptent des outils afin de permettre d'extraire et d'exploiter librement tout ou partie des bases de données contenant de telles données* » (souligné par l'Autorité).

75. Le Projet s'inscrit par conséquent dans un **objectif de maximalisation de la réutilisation** qui est mis en évidence dans les développements suivants. Autrement dit, **lorsqu'il légifèrera**, plutôt que de devoir penser à l'ouverture de données à la réutilisation (en transposition de la Directive Réutilisation ou en exécution du Règlement sur la Gouvernance des Données), **le législateur bruxellois devra à l'inverse s'interroger sur l'éventuelle nécessité de proscrire la réutilisation des documents concernés par la législation en cours d'adoption**.

76. Les **avis précédents de l'Autorité** doivent être consultés à titre préliminaires et à des fins de contextualisation s'agissant du premier régime de réutilisation.

77. Le second régime quant à lui, est lié au Règlement sur la Gouvernance des Données qui s'applique aussi à l'altruisme en matière de données. A titre préliminaire quant à ce dernier, **l'Autorité se réfère à l'avis (critique) rendu conjointement par le Comité Européen de la Protection des Données et le Contrôleur Européen de la Protection des Données** : EDPS-EDPB Joint Opinion 03/2021 *on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act*), 10 mars 2021 (ci-après, « **l'avis conjoint EDPB-EDPS** »)[122].

78. Trois caractéristiques de ce Règlement méritent d'être mises en évidence.

79. Premièrement, **le champ d'application du Règlement sur la Gouvernance des Données est défini en relation avec le champ d'application de la Directive Réutilisation des données[123]**. S'agissant de la réutilisation des données à caractère personnel, la Directive Réutilisation ne s'applique qu'aux données à caractère personnel qui seraient librement accessibles au public, sans restriction (de manière inconditionnée). Le Règlement sur la Gouvernance des Données **va plus loin** en s'appliquant à la réutilisation des autres données à caractère personnel qui se trouveraient dans les documents détenus par les autorités publiques, soit les « ***données protégées*** » visées par l'article 3, 1., du Règlement sur la gouvernance de la donnée.

[122] Disponible sur https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_en, dernièrement consulté le 4 octobre 2023.

[123] Voir les articles 1er, 2°, et 3, 1., d), et le considérant n° 10 du Règlement sur la Gouvernance des Données.

80. Deuxièmement, si ce Règlement va plus loin quant à son champ d'application en matière de réutilisation des données à caractère personnel, **il n'emporte toutefois aucune obligation de permettre la réutilisation de ces données protégées** : c'est au droit national qu'il incombe d'organiser la réutilisation de ces dernières[124].

81. Troisièmement, le Règlement sur la Gouvernance des Données est **sans préjudice du RGPD et du droit national en matière de protection des données** et prévoit explicitement en outre, **qu'en cas de conflit avec ceux-ci, ce sont ces derniers qui doivent prévaloir**[125].

II.5.2. Transposition de la Directive Réutilisation – articles C.IV.17 à C.IV.30

82. Le champ d'application, quant aux documents concernés, des dispositions du Projet transposant la Directive Réutilisation (articles C.IV.17 à C.IV.30), découle des articles C.IV.17, 1°, et C.IV.19. En particulier, l'article C.IV.19, § 2, 6° et 8°, énonce que le chapitre en cause ne s'applique pas aux deux types de documents suivants : « *aux documents dont l'accès est limité légalement notamment dans les cas où un intérêt personnel ou particulier est requis pour avoir accès aux documents* » ; « *aux documents dont l'accès est exclu ou limité en application de règles d'accès pour des motifs de protection des données à caractère personnel, et aux parties de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été définie par une norme législative comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement de données à caractère personnel ou comme portant à atteinte à la protection de la vie privée et de l'intégrité de la personne concernée, en particulier au regard des dispositions de droit de l'Union ou de droit national sur la protection des données à caractère personnel* » (souligné par l'Autorité).

83. Compte-tenu de l'articulation existant entre les règles régissant l'accès aux documents détenus par les autorités publiques et les règles relatives à la réutilisation de ceux-ci, l'Autorité renvoie à son commentaire précédent relatif à la nécessité de justifier ou pas d'un intérêt dans le cadre de la publicité passive de l'administration. Sur ce point, **le dispositif du Projet doit être adapté afin d'identifier clairement quelles données à caractère personnel sont susceptibles d'être réutilisées dans le cadre des règles transposant la Directive Réutilisation : il s'agit des données qui sont librement accessibles au grand public, sans aucune restriction[126], c'est-à-dire accessible de manière inconditionnée**. Les autres données à caractère personnel tombent dans le champ

[124] Voir l'article 5, 1., du Règlement sur la Gouvernance des Données. Le considérant n° 11 du Règlement sur la Gouvernance des Données exprime clairement que « *chaque Etat membre devrait par conséquent pouvoir décider si les données sont rendues accessibles à des fins de réutilisation, y compris en ce qui concerne les finalités et la portée de cet accès* ».

[125] Voir l'article 1er, 3., du Règlement sur la Gouvernance des Données.

[126] Doivent être incluses dans les hypothèses de restriction le cas visé par la Directive Réutilisation où une législation particulière qualifierait la réutilisation des données concernées comme incompatible avec la législation initiale sur la base de laquelle les données sont librement accessibles.

d'application du Règlement sur la Gouvernance des Données. Remarque : il semblerait que le champ d'application du Projet puisse à cette fin être rédigé en ayant recours au concept de « *donnée ouverte* »[127], le cas échéant adapté, consacré dans l'article A.III.1.13) du Projet, ce qu'il appartient au demandeur de vérifier[128].

84. Pour le reste, **l'Autorité semble comprendre du dispositif du Projet que la mise à disposition de données à des fins de réutilisation consiste en une « valorisation » des données au sens du Projet[129]**, et que par conséquent **c'est au responsable du traitement** qu'il appartiendra de déterminer si les données doivent être anonymisées, pseudonymisées ou autre, **en exécution de l'article C.III.14, § 3, du Projet**, dès lors que les dispositions relatives à la réutilisation des documents ne fixent pas le régime juridique du traitement des données à caractère personnel dans ce contexte.

85. A cet égard, tout d'abord, le dispositif du Projet **devrait expliciter que la communication de données à des fins de réutilisation consiste bien en une « *valorisation* »** soumise au régime consacré dans l'article C.III.14, § 3, al. 2, du Projet. Ensuite, cette disposition doit être **clarifiée** afin de ne présenter **aucun doute quant au régime de protection des données que le responsable du traitement doit appliquer**[130].

86. Selon le régime fixé, l'Autorité attire aussi l'attention du demandeur, *mutatis mutandis*, sur les considérants nos 23-24 de son **avis n° 144/2023.** Le considérant n° 24 précise notamment que : « *Dès lors que l'anonymisation ou la pseudonymisation de données nécessiteront en principe un traitement de données qui dépasse « le stade de la simple manipulation », l'Autorité est d'avis que le Projet doit clarifier la relation entre l'obligation d'une instance publique de mettre à disposition à des fins de réutilisation, des documents anonymisés ou pseudonymisés, d'une part, et d'autre part, l'absence d'obligation de cette même instance de mettre des documents à disposition sous une forme qui engendrerait un effort disproportionné dépassant le stade de la simple manipulation* […] » (mise en gras enlevée par l'Autorité dans le présent avis.

II.5.3. Exécution du Règlement sur la Gouvernance des Données – articles C.IV.31 à C.IV.32

[127] Voir la note de bas de page n° 5.

[128] L'article C.IV.17, 1° du Projet présente une certaine ambiguïté en ce qu'il s'énonce comme suit : « *la réutilisation des documents ouverts accessibles librement et des documents partageables accessibles aux conditions décrites dans le présent, titre conformément à la transposition de la Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte)* » (souligné par l'Autorité).

[129] Voir le considérant n° 20, dernier tiret et la définition du concept de « *valorisation* » reprise à la note de bas de page n° 11.

[130] Ce point est abordé ultérieurement, aux considérants nos 141 et s.

87. S'agissant de la **réutilisation des autres données à caractère personnel**, en exécution du Règlement sur la Gouvernance des Données, le Projet y consacre deux dispositions, à savoir l'article C.IV.31 reproduit ci-après, et l'article C.IV.32 organisant une voie de recours. Selon l'article C.IV.31 du Projet :

> « *§ 1er. Sans préjudice de dispositions particulières, le présent titre exécute le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724.*
>
> *§2. Les Autorités publiques permettent la réutilisation, à des fins commerciales ou non commerciales, des données protégées qu'elles détiennent et qui ont été produites aux seules fins de l'exercice de leurs missions de service public ou de leurs obligations d'intérêt général* » (souligné par l'Autorité).

88. En d'autres termes, le dispositif du Projet impose aux autorités publiques de manière tout à fait générale, et ce sans se référer aux règles relatives à l'accès à l'information, de mettre à disposition à des fins de réutilisation les données à caractère personnel qu'elles traitent dans l'exercice de leurs missions, à charge pour elles, *a priori*, de déterminer dans quelles conditions[131] (voir à ce sujet le **considérant n° 84, pertinent *mutatis mutandis* quant à l'article C.III.14, § 3, al. 2, du Projet**).

89. Dans le contexte **plus limité** du **champ d'application de la Directive Réutilisation**, l'Autorité avait considéré ce qui suit, aux considérants nos 9-11 de son avis n° 203/2021 précité :

> « *Dans ce contexte, la directive n'exclut par conséquent pas dans son principe, que des données à caractère personnel puissent être « réutilisées »[…]. Elle peut autrement dit sur le plan des principes, ouvrir la voie à deux grandes catégories de traitements de données : d'une part, l'anonymisation de données à caractère personnel en vue de permettre la réutilisation de documents ; d'autre part, la réutilisation de documents comportant des données à caractère personnel (pseudonymisées ou non). Ces deux catégories de traitements de données à caractère personnel constituent systématiquement des traitements de données ultérieurs devant satisfaire les conditions consacrées dans l'article 6, 4., du RGPD.*

[131] L'exposé des motifs de l'article C.IV.31 dispose que « *cette disposition ne nécessite pas de commentaire particulier* ». De nouveau, le régime juridique applicable à la réutilisation en exécution du Règlement découlerait de l'application de l'article C.III.14, § 3, dans la mesure où d'une part, la mise à disposition de données à des fins de réutilisation en exécution du Règlement sur la Gouvernance des Données constitue une hypothèse de « *valorisation* » des données, et d'autre part, les règles régissant la réutilisation dans le cadre de ce Règlement ne détermine pas de régime juridique de protection des données. Voir le considérant n° 20, dernier tiret et la définition du concept de « *valorisation* » reprise à la note de bas de page n° 11.

Un projet de norme du rang de loi tel que celui en cause dans le présent avis, pourra fonder en droit belge, le traitement de données par l'organisme du secteur public concerné consistant à anonymiser des documents contenant des données à caractère personnel, afin que ceux-ci puissent être mis à disposition à des fins de réutilisation. Les données une fois anonymisées sortant du champ d'application du RGPD, il n'y a alors plus, subséquemment, à assortir la réutilisation par le demandeur concerné, de conditions particulières liées à la protection des données. Et le traitement d'anonymisation des données sera justifiable au regard des exigences de l'article 6, 4., du RGPD[…].

Le projet pourra encore, ou des dispositions ad hoc consacrées dans des normes du rang de loi le cas échéant plus sectorielles, rechercher un équilibre plus complexe, en prévoyant les conditions auxquelles et dans lesquelles des données à caractère personnel pourraient être réutilisées par les personnes physiques ou morales qui le demandent, le cas échéant en excluant également les hypothèses de réutilisation de données à caractère personnel considérées comme incompatibles avec la protection des droits et libertés de personnes concernées. Dans une telle logique cependant, il conviendra en principe, systématiquement et in concreto, d'évaluer si les conditions prévues dans l'article 6, 4., du RGPD (analyse de compatibilité) sont rencontrées[…]*, et ce le cas échéant, compte-tenu des règles particulières applicables*[…]*. La réutilisation sera alors assortie de conditions liées au respect des règles de protection des données, et les données à caractère personnel seront le cas échéant pseudonymisées pour permettre la réutilisation* » (références omises et souligné par l'Autorité dans le présent avis).

90. Dès lors que par la disposition précitée le demandeur entend clairement soutenir l'objectif de la plus large réutilisation possible des informations détenues par les autorités publiques, y compris lorsque celles-ci contiennent des données à caractère personnel, **l'Autorité invite le demandeur à prendre connaissance des considérants nos 38-45 de son avis n° 167/2022**, également relatifs à la transposition de la Directive Réutilisation. Aux considérants nos 46 à 48 de cet avis, l'Autorité a précisé ce qui suit, dans une hypothèse où la **réutilisation des données est envisagée à la suite de l'application des règles relatives à l'accès à ces données** :

« *Ensuite, le chapitre 4 du projet impose de permettre la réutilisation des informations diffusées ou mises à disposition. A ce stade du traitement des données, lorsqu'est envisagée la réutilisation des données, il découle soit des règles régissant l'accès, soit des règles régissant la diffusion des informations (et ce, sous réserve des développements précédents), que le demandeur peut accéder à tout ou partie des informations souhaitées.*

Dans un tel contexte, l'Autorité est d'avis que le projet n° 1 peut laisser, sur le plan du principe, la responsabilité, en exécution du RGPD et en particulier des principes de finalité et de minimisation des données[…], *à l'organisme public concerné de déterminer si les données concernées peuvent être réutilisées moyennant pseudonymisation ou anonymisation, voire telles quelles.*

Elle souligne toutefois d'emblée que cet organisme exercera à ce stade une responsabilité potentiellement complexe et importante, et rappelle à l'attention du demandeur et des responsables du traitement concernés les principes suivants, au sujet de l'anonymisation et de la pseudonymisation » (référence omise et souligné par l'Autorité dans le présent avis).

91. Sur ce point de l'articulation des règles régissant l'accès et de celles régissant la réutilisation, l'article 3, 3., b), du Règlement sur la Gouvernance des Données précise que le Règlement est sans préjudice du droit de l'Union et du droit national en matière d'accès aux documents. En l'occurrence, **le dispositif du Projet doit prévoir clairement s'il prévoit une nouvelle voie d'accès aux documents (Option 1) et ce, aux fins de réutilisation, ou si la réutilisation n'est envisageable que suite à l'exercice d'une voie préexistante d'accès aux données (Option 2).**

92. L'Autorité souligne que **dans la seconde optique (Option 2 – voie d'accès préexistante)**, la responsabilité pesant sur l'autorité publique concernée est double :

- Il lui incombe de **vérifier les conditions d'application de la législation concernant l'accès** aux données à caractère personnel en cause (p. ex., le demandeur peut-il accéder à la liste nominative des responsables de service d'une direction générale d'une autorité publique ; peut-il accéder à une décision de justice intégrale dans laquelle était partie une autorité publique ; peut-il avoir accès au dossier reprenant la liste des missions à l'étranger réalisée par le directeur d'une administration ; etc.) ; et

- De **vérifier que la réutilisation des données envisagées est conforme aux articles 5, 1., b), et 6, 4., du RGPD** (étant entendu que le Projet, qui se borne à permettre la réutilisation de manière générale, ne peut être lu comme une disposition qui répondrait à des objectifs visés à l'article 23 du RGPD[132]). **Autrement dit, une analyse de compatibilité**

[132] S'il était nécessaire de le rappeler, au sujet du Règlement sur la Gouvernance des Données, le considérant n° 53 de l'avis conjoint EDPB-EDPS précité exprime confirme que « *in light of the objective and content of the Proposal, the EDPB and the EDPS consider that the Proposal cannot be invoked as Union law constituting a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) of the GDPR in order to ground the processing for a purpose other than that for which the personal data has been initially collected, where such processing is not based on consent, as per Article 6(4) of the GDPR* ».

est à mettre en œuvre, compte-tenu de la finalité poursuivie par la législation régissant l'accès.

93. Dans **la première optique (Option 1 – voie d'accès nouvelle et propre pour la réutilisation)**, la réutilisation des documents n'en demeurerait pas moins un traitement ultérieur de données. Cela étant précisé, **l'analyse de compatibilité à mettre en œuvre devra être réalisée compte-tenu de la finalité poursuivie par l'autorité publique dans le traitement des données concernées** (il s'agit autrement dit, de prendre en considération sa mission d'intérêt public).

94. Au considérant n° 77 de l'avis conjoint EDPB-EDPS, les institutions européennes sont **allées jusqu'à juger que** « *the EDPB and EDPS strongly recommend to amend the Proposal so as to clarify that the re-use of personal data held by public sector bodies may only be allowed if it is grounded in Union or **Member State law** which lays down **a list of clear compatible purposes for which the further processing may be lawfully authorised or** constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 of the GDPR* » (souligné et gras modifié par l'Autorité).

95. L'Autorité souligne qu'une telle approche, qu'elle a également évoquée[133], a pour mérite d'apporter une **plus grande sécurité juridique pour les responsables du traitement** (autorité publique et ré-utilisateur) **et les personnes concernées**.

96. Plus récemment, **en lien avec la question de savoir si les données à caractère personnel doivent être pseudonymisées ou anonymisées avant d'en permettre la réutilisation**, l'Autorité a exprimé la position suivante aux considérants nos 10-12 de son avis n° 144/2023 :

> « *Cela étant précisé, l'Autorité attire en outre l'attention du demandeur sur les **considérants nos 17-19 de son avis n° 203/2021** du 25 octobre 2021 concernant un projet de décret n° 2020/279 de la Commission communautaire française relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2021-196), selon lesquels :*
>
> > *« […] il importe de souligner que l'état de la technique et les techniques d'anonymisation sont évolutives, tout comme les données disponibles (publiquement ou pas) qui rendraient les données identifiables du point de vue des destinataires des données dé-identifiées (p. ex., nouvelles possibilités de réidentification des personnes concernées lorsqu'il y a eu une fuite de données, publication d'autres jeux de données qui n'étaient pas encore disponibles au moment de l'anonymisation, etc.[…]). Dans un*

[133] Voir le considérant n° 89, al. 4.

tel contexte, l'état anonyme ou non de données pourtant « anonymisées » et communiquées comme telles (à savoir, comme sortant du champ d'application du RGPD) variera avec le temps. De telle sorte qu'un traitement d'anonymisation des données à caractère personnel fondé sur la « dé-identification » des données (sur la base d'une des techniques renseignées plus haut – randomisation, etc.) qui sont ensuite communiquées comme telles aux demandeurs de réutilisations de données, pourrait amener le demandeur à partager des données qui deviendraient ré-identifiables sans que celui-ci ne puisse – a posteriori – limiter leur diffusion.

En outre, ces techniques pourraient limiter (potentiellement trop strictement, selon la nature des données originales et compte-tenu de la finalité de la réutilisation concernée – ce qui est à étudier au cas par cas,) les possibilités de traitement (et partant l'utilité) des données « anonymisées » pour les demandeurs de réutilisation et la société dans son ensemble.

*Partant, l'Autorité attire l'attention du demandeur sur **d'autres possibilités techniques existantes qui pourraient également contribuer à la réutilisation des données concernées, le cas échéant de manière plus efficiente,** en maintenant des conditions techniques contraignantes quant à l'utilisation des données qui peut être envisagée par le demandeur et en organisant différemment (plutôt qu'une simple communication des données dé-identifiées) la manière dont les données sont mises à disposition des demandeurs, comme par exemple via des services[134] » (mise en gras et souligné par l'Autorité dans le présent avis).*

***Dans une perspective plus globale** dans le domaine de la réutilisation des informations du secteur public, **l'Autorité attire l'attention du demandeur sur l'importance de prendre en considération ce type d'autres possibilités**. Dans ces hypothèses, plutôt que de prévoir la communication de données à caractère personnel (brutes, pseudonymisées, ou la communication de données rendues anonymes) au demandeur qui entend réutiliser les données, des **services d'accès sécurisé aux données concernées** sont offerts par une entité tierce (qui peut être un tiers de confiance[...]), à ce demandeur. De cette manière, tant d'un point de vue normatif (le traitement de données demeure soumis au RGPD) que technique, **un meilleur contrôle peut être garanti sur le traitement des données tout en permettant la réutilisation des données concernées**. De tels services pourraient*

[134] « *Voir par exemple https://www.casd.eu », dernièrement consulté le 20/09/2023. Voir également K. GADOUCHE, « The Secure Data Access Centre (CASD), a Service for Datascience and Scientific Research », 22/06/2021, disponible sur https://www.insee.fr/en/information/5014754?sommaire=5014796, dernièrement consulté le 20/09/2023* ».

ainsi contribuer à maximiser à la fois, les possibilités de réutilisation des données et les garanties pour les droits et libertés des personnes concernées.

En l'état de la technique, compte-tenu de la complexité liée à la mise en œuvre d'un processus optimal d'anonymisation des données au regard des risques de réidentification, ***l'Autorité est d'avis qu'il convient de privilégier ce type de services d'accès aux données en vue de leur réutilisation****, plutôt que de prévoir la communication de jeux de données (pseudonymisées ou rendues anonymes), s'agissant d'une méthode plus efficace pour garantir à la fois le contrôle sur le traitement des données et des possibilités de réutilisation de celles-ci* » (référence omise dans le présent avis).

97. L'Autorité observe au passage que l'article 5, 3., du Règlement sur la Gouvernance des Données **laisse la marge de manœuvre (et la responsabilité y liée) aux Etats membres pour prévoir une série d'exigences permettant de préserver le caractère protégé des données** (accès suite à anonymisation, accès via un environnement sécurisé fourni ou contrôlé par l'autorité publique concernée, accès dans les locaux où se trouve l'environnement sécurisé, etc.). **L'article C.V.13, 1°, du Projet peut être le cas échéant développé** afin d'organiser l'hypothèse des services d'accès sécurisés aux données.

98. Au passage, bien que ce concept ne soit pas repris dans le cadre des règles du Projet relatives à la réutilisation, l'Autorité observe que le Projet définit néanmoins le concept de **tiers de confiance**[135]. Elle attire l'attention du demandeur sur les **considérants nos 13-17 de son avis n° 144/2023**. Plus précisément, le considérant n° 17 de cet avis s'énonce comme suit :

« *Plus concrètement, à l'aune des cadres normatifs précités, et sans préjudice des considérations que l'Autorité estimerait utile d'émettre à l'avenir à ce sujet,* ***l'Autorité est d'avis que les éléments suivants sont pertinents dans le cadre de la conception de telles dispositions et des réflexions en la matière****, sous réserve de la possibilité de leur mise en œuvre au regard du droit européen (ce qu'il appartient au demandeur de vérifier) :*

- *La fixation de* ***conditions relatives à la relation entre l'autorité publique concernée et le demandeur d'un côté, et le tiers de confiance de l'autre****. A ce sujet, le tiers de confiance devrait notamment être indépendant de l'autorité publique et du demandeur de la réutilisation ;*

[135] Voir la note de bas de page n° 10.

- *La détermination des **responsabilités** des parties en cause au regard du traitement de données (pseudonymisation, anonymisation ou service d'accès sécurisé aux données). Notamment à ce sujet, compte-tenu de l'indépendance du tiers de confiance, de l'expertise spécialisée attendue de sa part ainsi que des obligations spécifiques qui lui incomberaient en la matière, du fait qu'il définira les caractéristiques essentielles (même s'il n'est pas exclu que l'autorité publique concernée soit également amenée à prendre certaines décisions dans le cadre de la mise en œuvre d'un processus d'anonymisation par exemple) des services qu'il offre, **l'Autorité est d'avis que le tiers de confiance devra être considéré comme le responsable conjoint du traitement** d'anonymisation ou de pseudonymisation des données, avec l'instance publique concernée ;*

- *La fixation de **conditions relatives au service offert/au traitement de données**. Par exemple, l'obligation de détruire les données une fois leur anonymisation réalisée peut être prévue, l'interdiction de principe des traitements de données en vue de réidentifier les personnes concernées, l'interdiction de traiter les données pour d'autres finalités, et l'obligation de rencontrer un niveau élevé de fiabilité. Dans ce contexte, l'Autorité est consciente de la difficulté d'assurer la mise en œuvre de garanties techniques et le cas échéant, procédurales également, dans le cadre d'un schéma de certification, élevées, et de permettre à la fois le développement de l'innovation en la matière, afin que les instances publiques puissent disposer d'une offre de services (de confiance) pertinente et suffisante. Il appartient au demandeur **d'assurer plus généralement que les conditions qu'il fixerait assurent le meilleur équilibre entre un niveau de garantie élevé et la possibilité d'innover et de développer des services en matière de pseudonymisation, anonymisation ou d'accès sécurisé aux données** ;*

- *La détermination d'obligations en matière de **transparence**. De telles obligations peuvent par exemple concerner la déclaration/notification des tiers de confiance et publication de l'identité de ceux-ci, et la réalisation d'audits externes[136]. Plus fondamentalement, s'agissant de l'anonymisation, sont pertinentes des **obligations de transparence relatives aux processus d'anonymisation et aux mesures qui sont mises en œuvre pour limiter les risques de réidentification, ainsi que les compromis réalisés dans ce cadre** ;*

- *La fixation de **conditions relatives au prestataire de service tiers de confiance**. De telles conditions porteraient notamment sur son niveau **d'expertise** dans le cadre du*

[136] Dans le domaine des élections sociales, voir par exemple le considérant n° 14 de l'avis n° 62/2023 du 9 mars 2023 *concernant un avant-projet de loi modifiant la loi du 4 décembre 2007 relative aux élections sociales, la loi du 20 septembre 1948 portant organisation de l'économie et la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail (CO-A-2023-030)*.

traitement de données (pseudonymisation, anonymisation, accès sécurisé aux données), au regard de l'état de la technique, et sur sa capacité financière ».

99. En conclusion, et compte-tenu des ambitions du Projet, l'Autorité est d'avis que **le régime juridique de réutilisation des données consacré dans l'article C.IV.31 du Projet doit être développé à l'aune des considérations précédentes**.

II.5.4. Publication de données à caractère personnel

100. L'article C.V.10, § 3, du Projet prévoit que « *Pour chaque jeu de données ayant fait l'objet d'une réutilisation, le Portail ouvert des données publiques indique le nombre et l'identité des réutilisateurs* ».

101. L'Autorité renvoie avant tout au **considérant n° 42** du présent avis, s'agissant de la publication de données à caractère personnel.

102. L'Autorité est d'avis **qu'*a priori*, la mesure de publicité en Projet pourrait être justifiée** s'agissant des hypothèses de réutilisation des données **au sens de la Directive Réutilisation et au sens du Règlement sur la Gouvernance des Données**, compte-tenu des possibilités ouvertes par ces textes. Une telle mesure de transparence est **de nature à renforcer efficacement la mise en œuvre** des règles de protection des données (y compris lorsque les données à caractère personnel ont été anonymisées avant réutilisation), dont l'information de la personne concernée. Sa **finalité**, qui doit être spécifiée, serait ainsi à tout le moins, d'informer les personnes concernées quant aux réutilisations qui sont mises en œuvre afin de faciliter l'exercice des droits dont elles jouissent en vertu du RGPD.

103. Cela étant précisé, l'article A.III.1.71 définit le concept de « *réutilisation* »[137] sans référence explicite à la transposition de la Directive Réutilisation des données et à l'application du Règlement sur la Gouvernance des Données, ou autrement dit, sans référence explicite aux demandes de réutilisation s'inscrivant dans le champ d'application de ces législations européennes[138]. Par conséquent, **il n'est pas exclu que « *l'utilisation par les personnes physiques* » de documents obtenus en**

[137] Comme suit :

« *utilisation par des personnes physiques ou morales de documents détenus par :*

a) des Autorités publiques, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les documents ont été produits, à l'exception de l'échange de documents entre des Autorités publiques aux seules fins de l'exercice de leur mission de service public, ou ;

b) des entreprises publiques, à des fins commerciales ou non commerciales autres que l'objectif initial de fournir les services d'intérêt général pour lequel les documents ont été produits, à l'exception de l'échange de documents entre des entreprises publiques et des Autorités publiques aux seules fins de l'exercice de leur mission de service public ».

[138] L'exposé des motifs indique néanmoins que la définition concernée « *transpose l'article 2, 11) de la Directive ISP* ».

exécution des règles régissant l'accès aux documents administratifs (transparence administrative passive) tombe dans le champ d'application de la mesure de publicité prévue par le Projet. **Or inversement, une telle mesure de publicité générale apparaîtrait disproportionnée**. Des mesures alternatives, dont le droit d'accès individuel des personnes concernées, pourraient suffire à assurer une transparente suffisante à l'égard des personnes concernées.

104. **L'Autorité réserve son analyse quant à une telle hypothèse mais semble comprendre de la logique du Projet que l'intention de son auteur n'est pas de l'inclure dans celui-ci.** Autrement dit, le demandeur pourrait se limiter à circonscrire le champ d'application de la mesure de publicité envisagée comme indiqué au considérant n° 102.

II.5.5. Altruisme en matière de données

105. Enfin, l'article C.IV.33 du Projet porte sur la question de l'altruisme en matière de données. Il dispose que :

> « *§ 1er. Sans préjudice de dispositions particulières, le présent titre exécute partiellement le Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724.*
>
> *§ 2 . Par l'intermédiaire du Point de contact de la Plateforme bruxelloise de la donnée, le gestionnaire de la Plateforme bruxelloise de la donnée organise l'altruisme en matière de données pour l'ensemble des Autorités publiques par la Communication des données à caractère personnel ainsi que toutes autres données qui seraient volontairement mises à disposition à des fins d'intérêt général* ».

106. L'Autorité souligne qu'en effet sur ce point, l'exécution du Règlement est partielle et que **l'altruisme en matière de données ne peut en l'état du dispositif du Projet être mis en œuvre**. En effet, il appartient au **droit national** des Etats membres notamment de fixer les objectifs d'intérêt général aux fins desquels l'altruisme en matière de données peut être permis[139].

II.6. COMMISSION D'ACCÈS AUX DOCUMENTS ADMINISTRATIFS ET AUX DONNÉES (« CADADO »)

II.6.1. Un organe de recours et d'avis différent d'une autorité de protection des données

[139] Voir l'article 2, 16), du Règlement sur la Gouvernance des Données. Voir également l'article 16 de ce même Règlement.

107. La CADADO est une **autorité administrative indépendante et impartiale** dont les membres sont désignés par le pouvoir exécutif[140]. Elle est composée de trois chambres, l'une relative à l'accès aux documents administratifs, une autre concernant la réutilisation de données et enfin, une troisième compétente pour le partage administratif. Le projet attribue à la CADADO une série de **compétences de recours** (notamment contre les rejets de demandes d'accès aux documents, contre les refus de rectification de données, contre les décisions d'une autorité publique relative au partage administratif des données ou à la réutilisation des données) **et d'avis** (également en matière de partage administratif de données et de réutilisation des données)[141]. Elle dispose aussi d'un pouvoir de réformation des décisions des autorités publiques, du pouvoir de communiquer elle-même des données ou documents[142] et de pouvoirs d'investigation et de contrainte[143]. L'exposé des motifs explique que le Projet notamment « *organise la fonction de la CADADo en tant que* ***gardienne de la légalité des flux de données au sein de la Région de Bruxelles-Capitale*** » (gras ajouté par l'Autorité).

108. L'Autorité prend acte du fait que **le Projet n'érige pas cette dernière en autorité de protection des données au sens du RGPD** et qu'il **supprime la Commission de contrôle bruxelloise** visée aux articles 31 et s. de l'ordonnance du 8 mai 2014 *portant création et organisation d'un intégrateur de services régional*.

II.6.2. Communication systématique de données à la CADADO

109. L'article B.II.19 du Projet prévoit une obligation à charge des autorités publiques concernées par les recours introduits auprès de la CADADO de communiquer systémiquement à celle-ci, dans les 7 jours ouvrables, le document ou l'information environnementale dont l'accès ou la rectification est sollicité, ou les données visées par le partage administratif ou les données visées par la réutilisation demandée.

110. **L'Autorité est d'avis qu'une telle communication systématique de données,** lorsqu'elle concerne les données à caractère personnel, **est disproportionnée**. Conformément aux principes de finalité et de minimisation des données, **c'est à la CADADO qu'il appartient d'exiger la communication des données si et quand celle-ci est nécessaire, aux fins de l'accomplissement de ses missions**. Il ne peut être exclu (au contraire) que la communication concrète des données à caractère personnel concernées *in* concreto, ne sera pas nécessaire à l'exécution de ses missions par la CADADO.

---

[140] Voir l'article B.II.3, § 3, du Projet, concernant l'indépendance et l'impartialité, et l'article B.II.7. qui prévoit que « *Les membres de la Commission sont désignés conjointement par le Gouvernement, le Collège réuni et le Collège pour un terme de 5 ans renouvelable une fois* ».

[141] Voir l'article B.II.3 du Projet.

[142] Article B.II.23 du Projet

[143] Voir l'article B.II.19 du Projet.

111. Le **même commentaire vaut *mutatis mutandis* pour l'article B.II.20, § 1er, al. 3, du Projet**.

II.6.3. Autres pouvoirs de la CADADO

112. L'article B.II.19, § 3, du Projet, prévoit que « *Si, malgré les pouvoirs de la Commission visés aux § 1er et 2, la Commission n'obtient pas les documents visés à l'alinéa 2, elle en informe sans délai selon le cas le Parlement de la Région, l'Assemblée réunie de la COCOM et l'Assemblée de la COCOF, de même que le Gouvernement, le Collège réuni et le Collège, qui fixent immédiatement de nouvelles sanctions et la procédure y afférente* » (souligné par l'Autorité).

113. L'Autorité n'est pas certaine de bien mesurer la portée de cette disposition. En tout état de cause, elle rappelle que si les pouvoirs et sanctions concernés entraînaient un nouveau traitement de données à caractère personnel (e.g. pouvoir de se faire communiquer des données à caractère personnel, d'auditionner des personnes concernées, etc.), les éléments essentiels de ce dernier devrait être consacrés dans une ordonnance ou un décret.

II.6.4. Avis de l'Autorité de Protection des Données

114. S'agissant du délai pour statuer sur les recours qui lui sont soumis, l'article B.II.20, § 2, 1°, du Projet, prévoit que le délai de 60 jours est suspendu « *lorsque la Commission a sollicité l'avis de l'Autorité de protection des données, jusqu'à la réception de cet avis* ».

115. Sur ce point, l'Autorité rappelle qu'elle n'est **consultable que selon les modalités consacrées dans la LCA**. A ce sujet d'une part, des demandes d'avis peuvent être introduites auprès du Centre de Connaissances de l'Autorité dans les conditions prévues à l'article 23 de la LCA (hypothèse du présent avis). La CADADO ne relève toutefois pas des autorités compétentes pour introduire une demande d'avis auprès de l'Autorité, conformément à cette disposition.

116. D'autre part, le Secrétariat général de l'Autorité peut également rendre un avis à l'attention d'un responsable du traitement, toutefois dans l'hypothèse limitée d'une analyse d'impact relative à la protection des données, à la suite d'une consultation par le responsable du traitement de l'Autorité de protection des données[144], lorsque le traitement concerné présente encore un risque résiduel élevé malgré les mesures de gestion des risques envisagés par le responsable du traitement[145].

[144] Article 20, § 1er, 3°, de la LCA.

[145] Voir notamment https://www.autoriteprotectiondonnees.be/professionnel/actions/consultation-prealable-aipd, et le guide publié par l'Autorité à l'adresse suivante https://www.autoriteprotectiondonnees.be/publications/guide-analyse-d-impact-relative-a-la-protection-des-donnees.pdf, dernièrement consultés le 08/09/2023.

117. **L'Autorité publique concernée** par le recours introduit auprès de la CADADO agit bien comme un responsable du traitement lorsqu'elle se décide à l'égard de l'accès à un document administratif ou à une information environnementale, lorsqu'elle réalise un partage administratif de données ou lorsqu'elle se prononce sur une demande de réutilisation d'informations.

118. La qualification de la CADADO, comme responsable du traitement à l'égard des traitements faisant l'objet des dossiers qui lui sont soumis, est toutefois *a priori* moins évidente. Cela étant précisé, celle-ci est impartiale et indépendante et l'article B.II.23, § 1er, du Projet précise que :

> « *La Commission dispose d'un pouvoir de réformation et peut elle-même accorder l'accès aux documents administratifs, aux informations environnementales ainsi que leur rectification ; elle peut elle-même accorder l'accès aux données visées par un partage administratif ou une réutilisation aux conditions qu'elle fixe. Dans ce cas, la Commission donne l'injonction à l'Autorité publique de se conformer à sa décision et de l'exécuter dans le délai qu'elle établit, lequel ne peut excéder 30 jours* ».

119. Dans ces conditions, la CADADO **peut effectivement également être considérée comme un responsable du traitement** du partage administratif et de la communication des données suite à une demande d'accès ou de réutilisation. Selon la manière dont elle agit, seule au moyen des données communiquées préalablement par l'Autorité publique, ou de concert avec l'autorité publique concernée à laquelle elle adresse une injonction, elle pourra respectivement être considérée comme responsable du traitement ou responsable conjoint du traitement (dans la mesure de son injonction). Dans ce contexte, **la CADADO est susceptible d'adresser une demande à l'Autorité de Protection des Données dans les conditions de l'article 20, § 1er, 3°, de la LCA**.

II.6.5. Publication des décisions de la CADADO

120. L'article B.II.24 prévoit ce qui suit :

> « *La Commission publie sur son site internet visés à l'article B.II.26, dans les 20 jours ouvrables de leur adoption, les décisions, avis et propositions qu'elle adopte.*
>
> *Sauf consentement préalable du requérant en vue d'une publication nominative, la Commission opère une anonymisation des décisions avant leur publication. Elle omet également toute information qu'elle jugera confidentielle* » (souligné par l'Autorité).

121. De nouveau, il appartient tout d'abord au dispositif du Projet de **fixer le régime juridique applicable au consentement concerné**, bien que le Projet définisse le concept de consentement

par référence au RGPD[146]. L'Autorité attire de nouveau l'attention du demandeur sur le fait qu'il sera crucial de correctement informer les personnes concernées à ce sujet et notamment compte-tenu du fait qu'une fois les données concernées mises à disposition via internet, il sera généralement illusoire de vouloir en maîtriser la circulation ultérieure.

122. Ensuite, cette mesure d'anonymisation (ou de consentement) n'est prévue qu'à l'égard des « *décisions* » de la CADADO. Il appartient au demandeur de **vérifier si les « *avis* » ou « *propositions* » de la CADADO sont susceptibles de contenir des données à caractère personnel** et, **dans l'affirmative, de mettre en œuvre des garanties similaires** pour les droits et libertés des personnes concernées.

II.7. GOUVERNANCE DE LA DONNÉE

II.7.1. Champ d'application (indéterminé) et portée obligatoire des règles du Code

123. La Partie C du Code est dédiée à la Gouvernance de la donnée et son champ d'application *ratione personae* est défini à la lumière du champ d'application de la Directive Réutilisation, comme l'explique l'exposé des motifs.

124. Avant tout, les intitulés des différents titres ou dispositions devraient être clarifiés **afin que ne subsiste aucun doute quant à la portée contraignante des règles consacrées dans la partie C du Code**. Ainsi, le livre C.II contient des principes généraux, soit : des **principes directeurs** qui, selon l'exposé des motifs, sont les « *clés d'interprétation des dispositions, droits et obligations conférées par le Code* » ; des **objectifs stratégiques**, à savoir, selon l'exposé des motifs, « *les standards, libellés en termes d'approche et de gouvernance, que les Autorités publiques doivent atteindre à long terme par l'application des dispositions du Code* » ; et des **objectifs opérationnels**, soit de nouveau selon l'exposé des motifs, « *les initiatives concrètes que les autorités publiques doivent adopter en vue d'atteindre les objectifs stratégiques* ». Les dispositions pertinentes **sont bien en principe rédigées comme des obligations**.

125. Tandis que le livre C.III, intitulé « *Obligations de gouvernance des Autorités publiques* », consacre diverses obligations dont l'application dépend du palier numérique dans lequel se trouvera une autorité publique, conformément à la décision du Gouvernement, du Collègue réuni et du Collège. L'appartenance à l'un ou l'autre des trois paliers prévus dépendra de seuils numériques à définir par le Gouvernement, le Collègue réuni et le Collège. **Le Projet ne détermine toutefois pas les dispositions qui s'appliqueront aux différents paliers** (sauf le premier palier auquel toutes les

[146] Voir les considérants nos 35-37 (également concernant l'éventuelle nécessité de mettre en place en outre, un droit d'opposition) et les considérants nos 141 et s.

obligations sont applicables) **et est explicitement incomplet sur ce point**[147]. **L'Autorité réserve par conséquent son analyse à ce sujet**.

II.7.2. Régimes juridiques applicables aux données

126. L'article C.II.15 du Projet est rédigé comme suit :

> « *Les Autorités publiques identifient le ou les régimes juridiques applicables aux données qu'elles détiennent.*
>
> *Les Autorités publiques tiennent compte de ces régimes juridiques dans les partenariats numériques visés à l'Art.C.III.2 dans lesquelles elles sont impliquées lorsqu'ils concernent tout ou une partie de la gestion des données* » (souligné par l'Autorité).

127. L'Autorité est d'avis qu'une telle disposition, se trouvant dans des décret et ordonnance conjoints (soit une norme du rang de loi), peut être une source d'insécurité juridique. L'Autorité est d'avis que les autorités publiques doivent **se conformer** aux régimes juridiques concernés, dans les partenariats numériques qu'elles concluent.

II.7.3. Réversibilité des données

128. L'article C.II.18 du Projet est rédigé comme suit :

> « *Les Autorités publiques recourent, lorsque cela est pertinent et de manière proportionnée au regard de l'objectif poursuivi, à la traçabilité et à la réversibilité des données, à l'exception des hypothèses pour lesquelles l'anonymisation est requise conformément à la législation ou à la réglementation applicable.*
>
> *Les Autorités publiques utilisent les outils informatiques permettant la traçabilité et la réversibilité des données tout en garantissant la protection de celles-ci* » (souligné par l'Autorité).

---

[147] L'article C.III.1. du Projet est rédigé comme suit :

« *Champ d'application du présent livres par palier*

Le Gouvernement, le Collège réuni et le Collège déterminent conjointement certaines catégories d'Autorités publiques en fonction de seuils numériques définis. À chaque seuil numérique correspond un palier numérique déterminant l'importance de l'activité numérique et la maturité numérique des Autorités publiques qui y sont regroupées.

Le premier palier est appelé à respecter l'ensemble des obligations du présent livre.

Le deuxième palier est soumis aux articles XXX.

Le troisième palier est soumis aux articles XXX ».

129. Avant tout, l'Autorité est d'avis qu'il convient de **clarifier dans le Projet ce que constitue la « *réversibilité* » des données**. D'un point de vue technique, ce ne sont pas les données elles-mêmes qui sont « réversibles » mais bien la fonction (le traitement) qui transforme ces données. Cela étant précisé, l'Autorité comprend du Projet que l'objectif poursuivi serait de pouvoir retrouver l'état antérieur d'une donnée lorsque celle-ci, au cours de son cycle de vie, a évolué et par conséquent, a été modifiée. Autrement dit, il s'agirait d'assurer l'historique de la donnée.

130. **Dans cette optique**, et, plus largement que ce que prévoit la disposition en projet, l'Autorité est d'avis que la réversibilité des données ne peut **pas non plus être possible lorsque les données doivent être détruites en vertu de la législation applicable ou même, lorsqu'elles ne peuvent plus être traitées par l'autorité publique responsable du traitement concernée**. Plus généralement et plus fondamentalement, l'Autorité rappelle que ce n'est pas parce qu'une donnée est réversible au sens juste exposé, que son été antérieur peut en tout état de cause être ré-établi. De manière générale, **la conservation de la donnée dans son (ou ses) état(s) antérieur(s) ou la remise d'une donnée dans un état antérieur,** notamment, **constituent des traitements de données à caractère personnel qui doivent être justifiés *in concreto* conformément au RGPD** (et au cadre normatif bruxellois ou autre, applicable).

131. C'est dans cette logique que semble bien s'inscrire l'article C.III.16, al. 2, 4°, du Projet, toutefois incomplet, en prévoyant que les données détenues par les autorités publiques doivent être « *réversibles, sans préjudice des dispositions réglementaires qui seraient applicables, tels que décrits à l'article B.II.XX.* » (Sic).

II.7.4. Typologie des catégories de données

132. L'article C.III.10, § 1er, du Projet prévoit que :

> « *Les données appartiennent, en fonction de leur régime de propriété, à l'une des catégories suivantes, qui déterminent les règles concernant leur utilisation :*
> *1° données à caractère personnel ;*
> *2° données exclusives ;*
> *3° données publiques ;*
> *4° données à forte valeur ;*
> *5° données d'origine privée* » (souligné par l'Autorité).

133. L'Autorité souligne que **ces catégories de données ne sont pas exclusives l'une de l'autre**. Ainsi par exemple, une donnée à caractère personnel peut être une donnée publique au sens du Projet.

Autrement dit, la disposition en projet doit être adaptée afin de refléter le fait qu'une donnée est susceptibles d'appartenir à plusieurs des catégories de données selon leurs régimes d'utilisation.

134. Pour le surplus, il appartient au demandeur d'éventuellement en tirer les conséquences dans le cadre de la mise en œuvre du Projet.

II.7.5. Valorisation des données d'usage

135. L'article C.III.13 du Projet est rédigé comme suit :

> « *Les Autorités publiques collectent et valorisent les données d'usage notamment en vue :*
>
> *1° d'identifier des profils d'usage, repérer des modes d'engagement avec les contenus ou les habitudes d'utilisation ;*
>
> *2° d'améliorer la lisibilité et l'accès à leurs services ;*
>
> *3° d'informer d'autres usagers ou citoyens que les usagers ou citoyens identifiés au départ des données d'usage déjà récoltées ;*
>
> *4° d'améliorer la représentation des usagers de leurs services ;*
>
> 5° *de protéger la vie privée des usagers en collectant les refus et les consentements en tant que donnée d'usage* »[148] (souligné par l'Autorité).

136. Premièrement, à partir du moment où cette disposition est susceptible de fonder une collecte de données à caractère personnel, l'Autorité rappelle que conformément aux principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution, celle-ci doit **fixer les éléments essentiels des traitements qu'elle permet et ce, de manière exhaustive**. Ainsi **premièrement,** le **terme « *notamment* » doit être omis de la disposition**.

137. Deuxièmement, l'Autorité note que la disposition en Projet n'est pour le reste pas claire et **ne répond pas aux exigences découlant des principes juste rappelés**. **Elle doit être développée et l'Autorité réserve son analyse à son sujet**. Les hypothèses visées aux 3° et 4° sont particulièrement floues. Outre la finalité de la disposition qui doit être explicitée à l'égard de l'ensemble des traitements concernés et de manière exhaustive, dans le dispositif du Projet, les catégories de personnes concernées doivent également être clairement identifiées, compte-tenu du fait que les concepts d'utilisateur, d'usager ou de citoyen apparaissant différents[149].

---

[148] Concernant les concepts de données d'usage et d'utilisateurs, voir la note de bas de page n° 6.

[149] L'exposé des motifs précise ce qui suit : « *Les données d'usage peuvent servir aux Autorités publiques qui les collectent essentiellement pour améliorer la qualité de leurs services numériques et la manière dont ils sont proposés.*

La valorisation des données d'usage permet aux Autorités publiques de personnaliser et de rendre plus ergonomiques ou « user friendly » leurs services numériques, dans une optique d'amélioration continue du service public ou des obligations d'intérêt général qu'elles assurent » (souligné par l'Autorité). L'Autorité observe au passage que le Projet ne définit pas le concept de « *service numérique* ».

138. A ce sujet, l'Autorité observe que le concept d'utilisateur repris dans la définition de la donnée d'usage (soit la personne qui a accès aux données) est bien distinct de celui d'usager dans la disposition précitée qui vise les personnes concernées par les données qui font l'objet d'un usage (d'un traitement) par leur utilisateur (un responsable du traitement).

139. L'Autorité relève que sur le plan du principe, que le concept de consentement du RGPD, auquel se réfère le Projet, est défini comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fasse l'objet d'un traitement* » (souligné par l'Autorité). Autrement dit en principe, plutôt que de « refuser », la personne concernée ne donnant pas son consentement ou demeurant indifférente, sera passive, de telle sorte que **la donnée pertinente sera l'absence de consentement plutôt que le refus**.

140. Par ailleurs, conformément aux principes de minimisation des données et d'*accountability*, **l'Autorité est d'avis que les données pertinentes et nécessaires à collecter sont les consentements exprimés,** et le cas échéant **dans une phase ultérieure du traitement,** selon le régime juridique applicable au consentement, **le retrait du consentement ou l'opposition au traitement de données**. La collecte de données à caractère personnel concernant les « *refus* » ou les consentements absents n'apparaît pas nécessaire.

II.7.6. Respect du droit des tiers dans la valorisation des données – consentement et al.

141. L'article C.III.14 du Projet prévoit que « *Dans le cadre de la valorisation des données qu'elles détiennent, les Autorités publiques respectent les droits des tiers sur les données protégées* ». Plus concrètement, s'agissant notamment de la protection des données, le paragraphe 3 de cette disposition s'énonce comme suit :

> « *Dans le cadre de la valorisation des données qu'elles détiennent, les Autorités publiques respectent la confidentialité des données protégées.*
>
> *Sauf disposition contraire applicable ou consentement des personnes concernées, les Autorités publiques adaptent leurs techniques, d'anonymisation ou de pseudonymisation au regard de la nature des données à caractère personnel traitées et des risques liés à leur valorisation* ».

142. Cette disposition **apparaîtrait d'une importance toute particulière dans la mesure où** elle déterminerait notamment le régime juridique applicable à la réutilisation des données à caractère

personnel[150]. Plus largement, **elle apparaît même être le régime juridique de protection des données applicable à défaut de législation particulière, aux hypothèses de valorisation des données**.

143. Par conséquent, l'Autorité est d'avis que **sa formulation doit être clarifiée afin d'indiquer une ligne de conduite sans ambiguïté au responsable du traitement**. Tel que formulé, en effet, l'article C.III.14 du Projet pourrait impliquer que sauf disposition contraire, le responsable du traitement **ne** peut **pas** communiquer des données à caractère personnel non pseudonymisées ou anonymisées aux fins de réutilisation (par exemple). L'exposé des motifs ne semble toutefois pas aller en ce sens et laisserait ce choix (communiquer ou non des données à caractère personnel brutes, pseudonymisées ou anonymisées) à l'appréciation du responsable du traitement[151]. Autrement dit, le dispositif du Projet devrait expliciter que le responsable du traitement doit déterminer si les données concernées doivent être pseudonymisées ou anonymisées et adapter ces traitements de données (pseudonymisation ou anonymisation) conformément aux risques liés au traitement de données envisagé, sauf application d'une disposition normative particulière.

144. **Dans ce cas cependant**, **l'Autorité invite le demandeur à s'interroger sur l'utilité de la disposition en projet et l'invite à mettre celle-ci en évidence** : en effet, l'application directe des règles du RGPD impose déjà au responsable du traitement de déterminer si les données doivent être pseudonymisées ou anonymisées pour la réalisation d'un traitement de données, et ce, compte-tenu notamment des risques pour les droits et libertés des personnes concernées. En l'absence de prescrit spécifique, l'on peut s'interroger sur l'utilité de l'article C.III.14 qu'il faudrait envisager d'introduire dans les travaux préparatoires à titre d'explication plutôt que dans le texte de loi.

145. C'est également dans ce contexte qu'il convient de prendre en considération les commentaires de l'Autorité relatifs à la mise en place éventuelle de **services d'accès sécurisé aux données**[152].

146. L'article C.III.14, § 2, al. 2, du Projet prévoit au sujet du **consentement** que « *Le cas échéant, et sans préjudice des dispositions d'autres réglementations applicables au traitement des données concernées, les Autorités publiques mettent en place un mécanisme de consentement ou d'autorisation dynamique* » (souligné par l'Autorité). L'exposé des motifs énonce ce qui suit à ce sujet :

[150] Voir les considérants nos 84 et 88.

[151] Il précise en effet que « *Le RGPD définit ces deux notions mais ne dit pas dans quel cas il faut y recourir. Pour l'application du présent Code et dans le cadre de la valorisation des données, ces méthodes doivent être appliquées en fonction des risques liés à l'utilisation ou la réutilisation des données visées. Ainsi, un partage administratif entre Autorités publiques n'implique pas les mêmes risques qu'une réutilisation* ».

[152] Voir le considérant n° 96.

« *L'alinéa 2 envisage la mise en place d'une méthode de consentement ou d'autorisation dite « dynamique ».*

Cette méthode, également utilisée dans d'autres parties du monde –- voir notamment l'exemple canadien repris i.a. dans S., Gagnon-Turcotte, M., Schulthorps, S. Coutts, Les partenariats de données numériques : mettre les bases d'une gouvernance de données collaborative dans l'intérêt public, Nord Ouvert, Montréal, 2021, pp. 60 et suivants –- garantit une réutilisation- correcte des données dans le temps. Ce mécanisme d'obtention du consentement ou de l'autorisation au cours de multiples phases de la collecte et du traitement des données offre généralement des options granulaires à différents moments du cycle de vie des données. Au fur et à mesure de l'évolution de la vie de la donnée, il convient de demander le consentement ou l'autorisation d'utilisation (ou la réutilisation) d'un même ensemble de données à caractère personnel ou d'autres données protégées (par exemple des secrets d'affaires ou des informations commerciales) chaque fois que les finalités de la collecte, du traitement, du partage de ces données changent.

Lorsque les Autorités publiques proposent cette fonctionnalité, ils veillent à ce que cette méthode « dynamique » du consentement ou de l'autorisation respecte les exigences du RGPD ou du DGA lorsque le partage concerne des données protégées. Lorsqu'un organisme public a l'intention de partager les données protégées pour une finalité différente de celle pour laquelle les données ont été collectées, il en informe préalablement les titulaires de droits sur ces données, en décrivant tout nouveau risque résultant de ce partage secondaire. Les personnes doivent avoir la possibilité de retirer leur consentement ou leur autorisation si elles ne sont pas ou plus favorables au partage secondaire de leurs données » (souligné par l'Autorité).

147. L'Autorité prend acte de cette disposition et de ces explications qui appellent les six commentaires suivants. Premièrement, le consentement de la personne concernée ne doit pas uniquement être de nouveau demandé lorsque la finalité du traitement change, il doit être **sollicité pour tout traitement de données à caractère personnel** fondé sur le consentement. Autrement dit, dans une hypothèse de réutilisation des données par exemple, il ne suffit pas que la personne concernée consente à une finalité spécifique de traitement (par exemple, peut-être sera-t-elle d'accord pour que le traitement soit réalisé par le responsable du traitement A mais pas par le responsable du traitement B).

148. Deuxièmement, le RGPD s'applique cumulativement au Règlement sur la Gouvernance des Données lorsque les données protégées concernées sont des données à caractère personnel.

149. Troisièmement, l'Autorité rappelle qu'un partage administratif de données, **soit un échange de données entre autorités publiques, ne pourra pas être fondé sur le consentement de la**

personne concernée (article 6, 1., a), du RGPD)[153], bien qu'il ne soit pas exclu qu'une place soit réservée à l'autonomie de la volonté de la personne concernée dans les hypothèses visées à l'article 6, 1., c) et e), du RGPD, afin de garantir la proportionnalité du traitement de données envisagé et de mettre en œuvre une garantie appropriée au profit des personnes concernées. Dans une telle hypothèse également, le régime juridique applicable à l'accord concerné doit être prévu par la norme spécifique concernée[154].

150. Quatrièmement et comme déjà indiqué précédemment, **le dispositif du Projet doit déterminer le régime juridique applicable au (retrait du) consentement[155]**.

151. Cinquièmement, l'Autorité est d'avis que **le dispositif du Projet** devrait lui-même reprendre l'obligation d'informer la personne concernée notamment « *en décrivant tout nouveau risque résultant* [du] *partage secondaire* » envisagé. Il s'agit d'une garantie utile en vue du respect des droits et libertés des personnes concernées.

152. Sixièmement, **l'Autorité recommande au demandeur de définir dans le dispositif du Projet, le « *mécanisme de consentement dynamique* »** dans le cadre du traitement de données à caractère personnel et ce, en tenant compte des considérations précédentes.

II.7.7. Recours dans le cadre de la valorisation des données

153. L'article C.III.14, § 4, du Projet, prévoit ce qui suit :

> « *Sans préjudice des droits des personnes concernées et des recours organisés par le RGPD, les Autorités publiques organisent les recours nécessaires afin que les titulaires de droits sur les données protégées puissent déposer plainte auprès des services ou des personnes compétentes au sein des Autorités publiques dès qu'ils estiment que leurs droits ne sont pas respectés ou sont menacés* » (souligné par l'Autorité).

154. L'Autorité comprend de l'exposé des motifs que cette disposition n'a pas vocation à s'appliquer pour ce qui concerne les contestations liées au traitement de données à caractère personnel. Conformément à l'exposé des motifs, cette disposition **n'est par conséquent pas seulement sans préjudice des droits des personnes concernées et des recours organisés par le RGPD contre les responsables du traitement, mais elle n'est également pas applicable aux plaintes**

---

[153] Voir les considérants nos 48-49.

[154] Pour une application récente, voir notamment l'avis de l'Autorité n° 83/2023 du 27 avril 2023 *concernant un avant-projet d'ordonnance modifiant l'ordonnance du 4 avril 2019 portant sur la plate-forme d'échange électronique des données de santé (CO-A-2023-147)*, considérants nos 26-28.

[155] Voir également le considérant n° 37.

relatives au traitement de données à caractère personnel. **Le dispositif doit être précisé en ce sens**.

155. L'Autorité réitère à l'attention du demandeur pour le surplus, les **principes de prévisibilité et de légalité** consacrés dans les articles 8 CEDH et 22 de la Constitution selon lesquels les éléments essentiels d'un traitement de données à caractère personnel doivent être fixés dans une disposition du rang de loi. En l'occurrence, compte-tenu de sa portée spécifique, la disposition en projet présente une certaine prévisibilité quant à la finalité des traitements (recours afin de faire valoir des droits sur les données protégées), aux (catégories de) données traitées (données relatives à la personne introduisant le recours, à la titularité des droits concernés, aux responsables du traitement concernés) et aux destinataires des données (les responsables du traitement concernés, y compris l'autorité publique concernée).

156. Néanmoins, d'une part, l'Autorité est d'avis qu'**une norme au moins réglementaire doit définir les recours** envisagés (et pas seulement les autorités publiques qui n'ont pas de pouvoir normatif).

157. Et d'autre part, le dispositif du Projet devrait également clarifier la **relation entre la voie de recours qu'il envisage et les éventuelles autres voies de recours disponibles aux ayants-droits concernés,** et identifier clairement **les actes concernés susceptibles du recours envisagé ainsi que l'autorité auprès de laquelle introduire le recours**. Il s'agit d'éléments essentiels liés à la finalité du recours concerné et qui sont également déterminant du point de vue de la personne concernée qui doit décider, selon ses impératifs et sa stratégie, si elle envisage l'introduction d'un recours contre un acte préjudiciable et quel recours.

158. C'est ainsi **principalement au Conseil d'Etat qu'il incombe de se positionner** au sujet des voies de recours à prévoir étant entendu que celles-ci ne sont pas applicables aux plaintes concernant le traitement de données.

II.7.8. Mise à jour des données

159. L'article C.III.16, als 3 et 4, est rédigé comme suit :

> « *Les Autorités publiques définissent la fréquence des mises à jour des données qu'elles détiennent.*
>
> *En tous les cas, les Autorités publiques :*
>
> *1° garantissent la plus haute fréquence de mise à jour compte tenu de la nature des données traitées et de l'objectif poursuivi ;*

2° documentent et publient la fréquence de mise à jour des données qu'elles détiennent ;

3° *garantissent que les titulaires de droits sur les données protégées puissent mettre à jour ou modifier les données à tout moment* » (souligné par l'Autorité).

160. L'Autorité souligne qu'une telle disposition **ne pourrait fonder à elle seule des collectes de données (ou croisement de données) en vue de mettre à jour les données concernées**, dans le cas ou de telles collectes de données (ou croisements de données) ne seraient pas déjà prévus par les règles régissant la mission d'intérêt public (ou l'obligation légale) de l'autorité publique concernée qui fonde le traitement de données au titre de l'article 6, 1., du RGPD. A titre illustratif, ce principe est particulièrement pertinent dans les hypothèses où les personnes concernées feraient l'objet d'un *screening*[156], hypothèse dans laquelle le responsable du traitement pourrait être tenté d'initier des traitements de données supplémentaires au motif que les données concernées doivent être à jour en application du RGPD.

161. Autrement dit, l'Autorité est d'avis que l'article C.III.16 du Projet doit également préciser que **la mise à jour des données ne peut être organisée que dans les limites permises par les règles régissant la mission d'intérêt public ou l'obligation légale servant de fondement au traitement de données concerné**. Il est dans ce cadre hautement probable que l'Autorité ne puisse par exemple pas collecter d'initiative à une fréquence fixée par elle, des données (auprès de la personne concernée par exemple, en la sollicitant périodiquement, ou ailleurs) en vue de mettre à jour les données qu'elle traite.

II.7.9. Données de référence

162. L'article C.III.17 prévoit notamment que les autorités publiques « *distribuent* » les données de référence. Dès lors que les données de référence peuvent concerner des personnes physiques[157], **l'Autorité réserve son analyse au sujet de cette disposition dont la portée est indéterminée** et doit être clarifiée (que signifie « distribuer » et à qui et pour quelle finalité).

163. L'article C.III.17 prévoit encore que les autorités publiques établissent des métadonnées fiables permettant notamment d'identifier les types de données à valoriser ou partager[158], la localisation des données, l'origine, des données, etc., et « *l'entité responsable de ces données* ». Compte-tenu de la

[156] Voir par exemple, l'avis de l'Autorité n° 245/2022 du 21 octobre 2022 *concernant un avant-projet de loi relative à l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Evaluation de l'Intégrité pour les Pouvoirs publics (CO-A-2022-248)*, considérants nos 51-56 ; avis n° 231/2021 du 3 décembre 2021 *concernant un avant-projet d'ordonnance concernant l'interopérabilité des systèmes de télépéage routier (CO-A-2021-227)*, considérants nos 62-63.

[157] Voir la note de bas de page n° 7.

[158] A noter que le partage serait un cas de valorisation.

portée de cette disposition, **l'Autorité est d'avis que l'identification des responsables du traitement devrait également être prévue**.

II.7.10. Modèles analytiques, algorithmes et intelligence artificielle

164. Article C.III.18 du Projet porte sur la « *gestion des modèles analytiques, des algorithmes et des systèmes exploitant l'intelligence artificielle* ». L'Autorité se limite à ce propos à se référer à la Proposition de Règlement du Parlement européen et du Conseil *établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union* et aux débats y liés[159], et à certaines positions qu'elle a déjà prises au sujet de la **prise de décision fondée exclusivement sur un traitement automatisé visée à l'article 22 du RGPD et du recours aux algorithmes, dont notamment** :

- Les considérants nos 15-17 de l'avis n° **231/2022** du 29 septembre 2022 *concernant un avant-projet de loi portant des dispositions fiscales et financières diverses, Titre 9 - Modifications de la loi du 16 décembre 2015 réglant la communication des renseignements relatifs aux comptes financiers, par les institutions financières belges et le SPF Finances, dans le cadre d'un échange automatique de renseignements au niveau international et à des fins fiscales, article 85 (CO-A-2022-226)*, où l'Autorité relève notamment « *qu'une présélection de contribuables en vue d'un contrôle plus approfondi réalisée par un algorithme demeure une décision automatisée notamment lorsque l'intervention humaine envisagée se limite à prévoir le simple entérinement systématique de la présélection par un agent. Dans une telle situation en effet, l'intervention humaine n'est pas liée au processus décisionnel qui demeure le fait exclusif de l'algorithme »* ; au considérant n° 18 du même avis, l'Autorité relève en outre « *concernant le traitement de données de sélection qui sera mis en place (soit, l'analyse de risque et les critères déclenchant un contrôle),* [qu']*il convient de recourir dans ce cadre à des paramètres[…] et leurs combinaisons dont il est établi qu'ils présentent une corrélation significative avec la fraude recherchée. Ceci est déterminant quant à la proportionnalité du traitement envisagé et quant à la qualité des données traitées, le traitement devant être efficace dans l'accomplissement de la finalité qu'il poursuit. Ainsi par exemple, déterminer de mauvais indicateurs de fraude en vue d'identifier les contribuables requérant un contrôle approfondi implique le traitement de données inadéquates et non pertinentes contraire à l'article 5, 1., c), du RGPD. Il est nécessaire dans ce contexte de mettre en place une phase de test préalablement à la mise en œuvre du traitement* » (gras enlevé dans le présent avis).

[159] COM (2021) 206 final. Voir également https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence, dernièrement consulté le 10/10/2023).

- Le considérant n° 13 de l'avis n° **203/2022** du 9 septembre 2022 *concernant un avant-projet de loi portant des dispositions fiscales et financières diverses - article 76 (CO-A-2022-158)*, insiste sur l'importance de la transparence quant aux données à caractère personnel traitées pour entraîner l'algorithme, quant aux critères de qualité qui seront utilisés, et quant aux conséquences concrètes pour les personnes concernées lorsqu'elles sont soupçonnées d'une éventuelle fraude (le dossier concernait la fraude fiscale) sur la base des résultats des algorithmes ;

- Le considérant n° 46 de l'avis de l'Autorité n° **135/2020** du 11 décembre 2020 concernant *la proposition de loi (Doc. parl., 55, 0642/006) modifiant la loi du 13 juin 2005 relative aux communications électroniques en ce qui concerne l'octroi automatique du tarif social (CO-A-2020-135)*, où est illustrée une autre mesure appropriée (en l'occurrence, un système d'*opt-out*) pour la sauvegarde des droits et libertés des personnes concernées dans un domaine particulier ;

165. L'Autorité rappelle à ce sujet que l'article 22, 1., du RGPD sera inapplicable dans le cadre des traitements de données réalisés par des autorités publiques, uniquement lorsque le droit national (ou le droit de l'Union) l'autorise et que des mesures y sont déterminées pour la sauvegarde des droits et libertés et des intérêts légitimes des personnes concernées. A ce sujet, il est clair que **si l'article C.III.18 du Projet contribue à la mise en place de telles mesures, il ne peut pas lui-même suffire en tant que disposition permettant de déroger à l'article 22, 1., du RGPD**.

166. A ce propos, le Projet devra **toujours être lu conjointement avec le cadre normatif définissant la mission d'intérêt public ou l'obligation légale incombant à l'autorité publique concernée**, étant entendu que c'est ce cadre normatif qui **autorisera ou non** la prise de décision individuelle automatisée, et encadrera celles-ci de **mesures complémentaires spécifiques au domaine qu'il réglemente** (en complément de l'article C.III.18 du Projet) et de nature à sauvegarder les droits et libertés des personnes concernées.

II.8. RESPONSABILITÉS AU REGARD DU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

167. L'Autorité rappelle à titre préliminaire sa pratique d'avis concernant la détermination des responsabilités au regard du traitement de données à caractère personnel : une autorité publique (ou une entité privée) est en principe responsable du traitement de données nécessaire à la mise en œuvre de la mission d'intérêt public qui lui incombe (ou qui relève de l'autorité publique dont elle est

investie)[160], ou nécessaire à l'obligation légale qui la lie[161], en vertu de la norme concernée[162]. Récemment, elle a de nouveau appliqué ces principes dans le cadre de l'échange de données entre autorités publiques, **aux considérants nos 7 et s. de son avis n° 143/2023**.

168. L'Autorité est d'avis que la **portée transversale du Projet**, qui a vocation à s'appliquer à l'ensemble des traitements de données fondés dans l'ordre juridique bruxellois, **peut se prêter à une formulation dans le dispositif du Projet, du principe d'identification des responsables du traitement juste rappelé par l'Autorité**, **sans préjudice des décrets ou ordonnances applicables par ailleurs[163]**. Dans le cadre du Projet et des législations qui lui seront concomitamment appliquées, l'autorité publique concernée sera le cas échéant, débitrice d'obligations spécifiques concernant le traitement de données lui-même, ou plus généralement, devra traiter des données à caractère personnel aux fins de l'exécution de ses missions d'intérêt public qui de nouveau, pourront elles-mêmes être liées au traitement de données.

169. Le Projet lui-même contient une série de dispositions qui fixent des obligations/responsabilités en relation avec le traitement de données, sans pour autant en l'état, systématiquement déterminer les responsabilités au regard du traitement de données à caractère personnel. Ce à quoi il convient pourtant de procéder, **à l'égard des rôles définis dans le Projet**[164].

170. L'hypothèse du CIRB (PARADIGM) constitue un bon exemple d'une institution chargée d'obligations et missions en lien direct avec le traitement de données, tant et si bien que le Projet sur ce point, impute à l'occasion au CIRB (PARADIGM) une responsabilité au regard du traitement de données à caractère

---

[160] Article 6, 1., e), du RGPD.

[161] Article 6, 1., c), du RGPD.

[162] Voir notamment : avis de l'Autorité n° 83/2023 du 27 avril 2023 *concernant un avant-projet d'ordonnance modifiant l'ordonnance du 4 avril 2019 portant sur la plate-forme d'échange électronique des données de santé (CO-A-2023-147)*, considérant n° 11 ; avis n° 129/2022 du 1er juillet 2022 *concernant les articles 2 et 7 à 47 d'un projet de loi portant des dispositions diverses en matière d'Economie*, considérants nos 42 et s. ; l'avis n° 227/2022 du 29 septembre 2022 *concernant un avant-projet de décret relatif aux données ouvertes et à la réutilisation des informations du secteur public (CO-A-2022-209)*, considérants nos 17-23 ; avis n° 131/2022 du 1er juillet 2022 *concernant un projet de loi portant création de la Commission du travail des arts et améliorant la protection sociale des travailleurs des arts*, considérants nos 55 et s. ; l'avis n° 112/2022 du 3 juin 2022 *concernant un projet de loi modifiant le Code pénal social en vue de la mise en place de la plateforme eDossier*, considérants nos 3-41 et 87-88 ; avis n° 231/2021 du 3 décembre 2021 *concernant un avant-projet d'ordonnance concernant l'interopérabilité des systèmes de télépéage routier*, considérants nos 35-37 ; l'avis n° 37/2022 du 16 février 2022 *concernant un avant-projet de décret instituant la plateforme informatisée centralisée d'échange de données 'E-Paysage'*, considérant n° 22 ; l'avis n° 13/2022 du 21 janvier 2022 *concernant un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale relatif à l'octroi de primes à l'amélioration de l'habitat et un projet d'arrêté du Gouvernement de la Région de Bruxelles-Capitale modifiant l'arrêté du Gouvernement de la Région de Bruxelles-Capitale du 9 février 2012 relatif à l'octroi d'aides financières en matière d'énergie*, considérants nos 9-17.

[163] Une telle approche contribue d'ailleurs à prendre en compte la préoccupation suivante, exprimée dans l'exposé des motifs :

« *Des données à caractère personnel seront traitées dans le cadre des services de la Plateforme. Il est nécessaire, au regard des dispositions applicables en la matière et notamment du RGPD, de prévoir le rôle que le gestionnaire endosse.*

Ce rôle n'est pas similaire en fonction des services envisagés et est éminemment casuistique : il serait disproportionné de prévoir un listing de chacun des traitements effectués dans le cadre de la Plateforme et le rôle correspondant dans le cadre du présent Code » (souligné par l'Autorité). L'Autorité ne partage ainsi pas cette analyse et se réfère aux développements repris dans le corps de l'avis au sujet de la désignation des responsables du traitement, à cet égard.

[164] Qui le cas échéant, peuvent aussi être des préposés du responsable du traitement.

personnel (au sujet des traitements du Centre d'intégration par exemple)[165]. À son sujet en particulier, **compte-tenu de son rôle central et incontournable, le Projet ne doit laisser subsister aucun doute quant aux responsabilités du CIRB (PARADIGM) au regard du traitements de données à caractère personnel**, ce qui implique notamment qu'il soit toujours possible de déterminer si le CIRB (PARADIGM) est tenu ou pas, et dans quelle mesure, de se soumettre aux instructions des autorités publiques concernées en matière de traitement de données à caractère personnel.

171. L'Autorité rappelle que selon le RGPD, le sous-traitant agit pour le compte du responsable du traitement, ne traite les données que sur instruction documentée du responsable du traitement et ne peut pas déterminer les finalités et les moyens du traitement (sauf à être requalifié en responsable du traitement)[166]. **Lorsque le Projet attribue une responsabilité de sous-traitant au CIRB (PARADIGM)[167]**, il convient qu'il y procède de manière précise et cohérente, et qu'il garantisse qu'aux fins de sa mise en œuvre, **le CIRB (PARADIGM) soit tenu d'agir, dans le cadre du traitement de données à caractère personnel, conformément aux instructions des autorités publiques qui recourent à ses services** (Catalogue des données[168], Portail ouvert[169] des données et Centre d'exploitation et d'analyse des données[170]).

172. Enfin, dès lors que le Projet ne prévoit pas de manière générale l'application des définitions du RGPD, il convient qu'il spécifie **l'application des définitions des concepts de responsable du traitement et de sous-traitant visées à l'article 4, 7) et 8), du RGPD**.

---

[165] Les alinéas 1er et 2 de l'article C.V.4 sont rédigés comme suit :

« *Le gestionnaire de la Plateforme bruxelloise de la donnée agit en tant que responsable de traitements pour les traitements des données à caractère personnel nécessaires à la gestion technique de la Plateforme ainsi que pour l'ensemble des traitements du Centre d'intégration.*

Le gestionnaire de la Plateforme bruxelloise de la donnée agit pour le compte des Autorités publiques en tant que sous-traitant pour les services du Catalogue, du Portail ouvert des données publiques et du Centre d'exploitation et d'analyse des données ».

L'exposé des motifs précise ce qui suit :

« *En revanche, en ce qui concerne particulièrement le Centre d'intégration, le gestionnaire définit aussi les moyens pour le recours aux services. Partant, il est, pour cette partie de la Plateforme uniquement, au moins coresponsable ou responsable du traitement* ».

Le Centre d'intégration est visé par l'article C.V.7 du Projet et permet d'assurer les partages administratifs. La fonction d'intégrateur de services bruxellois est définie dans l'article C.V.8. du Projet. **Sur la responsabilité conjointe d'un intégrateur de services et du responsable du traitement d'une source authentique de données**, voir le considérant n° 12 de l'avis n° 143/2023.

[166] Article 4, 1., 8), et 28, 3., a), et 10., du RGPD.

[167] La seule hypothèse identifiée par l'Autorité est citée à la note de bas de page n° 165.

[168] Celui-ci est prévu par l'article C.V.9 du Projet. **Cependant, rien dans cette disposition ne laisse comprendre que ce catalogue comportera des données à caractère personnel** et l'Autorité part du principe qu'il en est ainsi. Par conséquent, elle n'est pas certaine de percevoir la nécessité d'identifier le CIRB (PARADIGM) comme sous-traitant au regard du Catalogue de données.

[169] Visé par l'article C.V.10 du Projet.

[170] Quant à ce centre en particulier, voir les considérants nos 173 et s. Bien que l'Autorité ne se prononce pas à son sujet, dès lors que le Projet doit être développé sur ce point, l'Autorité doute que dans ce contexte, le CIRB (PARADIGM) agisse comme un simple sous-traitant.

II.9. CENTRE D'EXPLOITATION ET D'ANALYSE DES DONNÉES

173. C'est l'article C.V.11 qui détermine la « *Création et* [les] *objectifs* » du Centre d'exploitation et d'analyse des données comme suit :

> « *Il est créé un Centre d'exploitation et d'analyse des données.*
>
> *L'objectif du Centre d'exploitation et d'analyse des données est de proposer, notamment aux Autorités publiques, des services facultatifs visant la collecte, le stockage, le traitement et la consommation de données* » (souligné par l'Autorité)[171].

174. Une telle disposition **ne répond manifestement pas aux exigences de prévisibilité et de légalité consacrées dans les articles 8 CEDH et 22 de la Constitution** et ne peut par conséquent pas fonder le traitement de données à caractère personnel. Pour permettre le traitement de données à caractère personnel, la disposition en projet doit être significativement modifiée et **l'Autorité réserve son analyse sur ce point**.

II.10. DURÉE DE CONSERVATION DES DONNÉES

175. Le caractère transversal du Projet implique que ce dernier ne sera généralement pas le seul à prendre en considération s'agissant de la durée de conservation des données. Cela étant précisé, et le cas échéant en se référant à des dispositions applicables par ailleurs (selon par exemple, les partages administratifs de données), **l'auteur du Projet doit être en mesure de fixer des délais de conservation des données par le CIRB (PARADIGM), acteur central du dispositif, pour l'ensemble des traitements réalisés par celui-ci, fût-ce à l'occasion, de manière fonctionnelle[172]**.

---

[171] L'exposé des motifs énonce ce qui suit à ce sujet :

« *Le Centre d'exploitation et d'analyse des données regroupe l'ensemble des services et solutions facultatives offertes par le CIRB (PARADIGM) aux autorités publiques. Il est composé de plusieurs outils pour stocker, traiter et analyser les données.*

Il s'agit, à ce stade, de solution d'hébergement, de services d'analyse d'usage (analytics) et des services basés sur l'intelligence artificielle. Toutefois, le gestionnaire de la plateforme n'offre que des services, les questions relatives à la nature des données, à la sécurité et aux accès sont de la responsabilité exclusive de l'autorité qui fait appel aux services facultatifs offerts.

Le CIRB (PARADIGM), compte tenu de son expertise technologique, assiste néanmoins l'autorité publique dans les choix à prendre en fonction de la nature de l'opération à réaliser.

Néanmoins, le Centre d'exploitation et d'analyse des données a vocation, dans le futur, à proposer de nouveaux services facultatifs. Dans le cas où des services seraient rendus obligatoires, une modification du présent Code paraît nécessaire » (souligné par l'Autorité).

L'Autorité souligne que le caractère facultatif des services concernés ne dispense pas le législateur bruxellois de fixer les éléments essentiels des traitements de données à caractère personnel qui seraient envisagés.

[172] C'est-à-dire, le cas échéant, moyennant renvoi aux règles régissant par ailleurs les traitements de données concernés.

176. L'article C.V.4 du Projet prévoit ce qui suit, s'agissant de la durée de conservation des données par le CIRB (PARADIGM) (soit, le gestionnaire de la Plateforme bruxelloise de la donnée) :

> « […]
>
> *En ce qui concerne les données à caractère personnel nécessaires à la gestion technique de la Plateforme ainsi que pour l'ensemble des traitements des données à caractère personnel réalisés par le Centre d'intégration, les données sont conservées 10 ans après la fin du traitement.*
>
> *Sans préjudice d'autres dispositions légales notamment relatives à l'archivage historique, les données techniques nécessaires au fonctionnement des autres services de la Plateforme sont conservées 6 mois après la fin du traitement.*
>
> *Les données sont détruites à l'échéance des délais précités sauf si celles-ci sont nécessaires dans le cadre d'un examen de suivi ou à des fins historiques, statistiques ou scientifiques dans le respect de la législation relative à la vie privée.*
>
> *Pour ce faire, les données à caractère personnel sont rendues anonymes dès que leur individualisation n'est plus nécessaire pour la réalisation des finalités pour lesquelles elles ont été collectées.*
>
> *Les données pourront être communiquées à toute institution désignée par le Gouvernement, le Collège réuni et le Collège en vue de leur traitement ultérieur à des fins historiques, statistiques et scientifiques* » (souligné par l'Autorité).

177. L'exposé des motifs précise ce qui suit au sujet de cette disposition :

> « *Cela étant, une distinction du délai d'archivage existe entre les données techniques relatives au fonctionnement du Centre d'intégration et celles des autres services.*
>
> *Vu la caractère personnel des données mises à disposition par le Centre d'intégration, un délai de conservation des données d'accès plus long se justifie dès lors qu'une atteinte à celles-ci, pourraient entraîner des risques plus importants pour les personnes concernées.*
>
> *Ce délai est moindre (6 mois) dès lors qu'il concerne des accès à des jeux de données ne présentant pas de réel danger pour la vie privée (ex : données en open data)* ».

178. L'Autorité souligne d'emblée que **la disposition en projet manque de clarté et que le Projet ne justifie pas la durée de conservation des données qu'il fixe**. **L'Autorité réserve par conséquent son analyse** au sujet de la question du délai de conservation des données par le CIRB (PARADIGM) dans le cadre du fonctionnement des services de la Plateforme bruxelloise de la donnée. **La disposition en Projet doit être clarifiée et doit permettre** de distinguer clairement les délais de conservation des données (le cas échéant, maximums) par le CIRB (PARADIGM), selon les services concernés, et, dans le cadre d'un service concret, selon d'une part, que les données en cause sont l'objet du traitement de données à caractère personnel réalisé par l'autorité publique concernée et le CIRB (PARADIGM) dans le cadre du service, ou d'autre part, sont les données collectées à propos de ce traitement, notamment pour assurer la mise en œuvre des mesures techniques et organisationnelles permettant de garantir la sécurité du traitement (logs et accès, etc.).

179. Par exemple, si le Centre d'intégration assure techniquement un partage administratif via un canal qu'il fixe[173], à la demande d'une autorité publique[174], il n'y a *a priori* aucune raison qu'il conserve la donnée à caractère personnel échangée plus longtemps que ce qui est nécessaire à son échange *in concreto*, entre les autorités publiques. Une fois la donnée concernée reçue, le partage est terminé. En revanche, les données concernant la **traçabilité des opérations de traitement[175]** (de l'échange de données en l'occurrence), cruciales pour une mise en œuvre effective des règles de protection des données et l'audit du système d'information concerné, doivent être conservée pour une durée plus longue. A cette fin, un délai de conservation des données de 10 ans au moins est justifiable.

180. Le **Projet doit en outre clarifier ce que constitue un** « ***examen de suivi*** », ce concept étant indéfini. En l'état, une telle finalité ne pourrait justifier la conservation des données au-delà de leur délai original de conservation. L'Autorité **réserve par conséquent son analyse sur ce point**.

181. Compte-tenu de l'ingérence importante que le Projet entraîne dans les droits et libertés des personnes concernées et du rôle central du CIRB (PARADIGM), **l'autorité souligne tout d'abord qu'elle est favorable à l'approche suivie par le Projet qui consiste à imposer la destruction des données une fois leur délai de conservation (de traitement) arrivé à son terme**. Il s'agit d'une garantie importante pour les droits et libertés des personnes concernées. Cette garantie consistant à prévoir la destruction des données au terme d'un (ou plusieurs) délai(s) établi(s) clairement dans la norme du rang de loi est d'autant plus importante que le CIRB (PARADIGM) est un acteur central du traitement de données dans l'ordre juridique bruxellois, comme cela a été mis en évidence précédemment.

---

[173] Article C.V.7 du Projet.

[174] Article C.V.8, al. 2, 5°, du Projet.

[175] Accès à la donnée, modification de la donnée, etc.

182. **Cela étant précisé, l'article C.V.4 du Projet prévoit cependant des traitements ultérieurs** de manière générale, à des fins historiques, statistiques ou scientifiques, et ce de manière ambigüe, sans qu'il soit clairement défini quand lorsque les données doivent être rendues anonymes. Ainsi notamment, le doivent-elles lorsqu'elles sont communiquées à ces fins, à une « *institution* » désignée par le Gouvernement ? **L'Autorité est d'avis que l'article C.V.4 du Projet doit être clarifié et réserve son analyse à son sujet**. En passant, elle note que l'exposé des motifs est muet à ce sujet.

183. La disposition en Projet prévoit des traitements de données à caractère personnel et par conséquent, **les éléments essentiels de ces traitements doivent être fixés dans le dispositif du Projet conformément aux principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution**.

184. Notamment, la disposition en projet doit clairement identifier les (catégories de) données qui sont susceptibles de faire l'objet du traitement ultérieur de données envisagé et les responsables du traitement. En effet, la justification de la nécessité de la disposition en projet sera significativement différente selon qu'il s'agisse de réaliser des statistiques ou recherches en lien avec les activités et le fonctionnement de la Plateforme bruxelloise de la données (autrement dit, des statistiques et recherches portant sur les données générées par le fonctionnement de la plateforme) ou en lien avec les autorités publiques et les données concrètes traitées par celles-ci via les services de la plateforme. Cette deuxième hypothèse nécessitera en tout état de cause une justification particulière dès lors que ces mêmes recherches ou statistiques sont susceptibles de pouvoir être réalisées au niveau (à partir de) l'autorité publique concernée. Toujours sur le plan des statistiques, l'encadrement par une norme du rang de loi des traitements envisagés variera selon les statistiques envisagées[176].

185. Dans la justification de la nécessité de prévoir les traitements ultérieurs de données envisagés, il convient encore de **prendre en compte le fait que le Projet lui-même organise de manière très large l'accès aux informations détenues par les autorités publiques bruxelloises, ainsi que la réutilisation de celles-ci**, ces hypothèses pouvant couvrir également des cas de recherches scientifiques ou de statistiques. **L'exposé des motifs doit développer, à l'aune de ces considérations, la justification de la nécessité de l'article C.V.4, dans un cadre de recherche statistique ou scientifique**.

[176] Pour une illustration d'une hypothèse dans laquelle aucun encadrement normatif spécifique n'est nécessaire, voir l'avis n° 110/2022 du 3 juin 2022 *concernant un projet d'arrêté royal relatif à la formation des utilisateurs professionnels de produits biocides* (CO-A-2022-106), considérant n° 14. Pour une illustration d'un traitement nécessitant un encadrement légal particulier, voir l'avis n° 211/2022 du 9 septembre 2022 *concernant un projet d'arrêté royal portant modification de l'arrêté royal du 22 février 2017 portant création du Service public fédéral Stratégie et Appui (CO-A-2022-187)*. Pour une illustration dans le domaine spécifique de la statistique publique, voir l'avis n° 35/2023 du 9 février 2023 *concernant un projet de décret introduisant dans le Code wallon de l'Action sociale et de la santé des dispositions relatives aux programmes de médecine préventive* (CO-A-2022-295), considérants nos 56-59 ; l'avis n° 127/2021 du 28 juillet 2021 *concernant l'avant-projet de loi modifiant la loi du 4 juillet 1962 relative à la statistique publique (CO-A-2021-127)*.

186. De nouveau compte-tenu de l'ingérence importante dans les droits et libertés entraînée par le Projet, l'Autorité est d'avis que le Projet doit clarifier qu'en toute hypothèse, les données doivent être **rendues anonymes** à la fin envisagée.

II.11. DÉSIGNATION D'URBIS COMME BANQUE DE DONNÉES ISSUES DE SOURCES AUTHENTIQUES

187. Le Projet contient un Titre III « URBIS ». Ce **titre distinct du Code comprend des définitions propres des concepts** notamment de sources authentiques et banque de données issues de sources authentiques pourtant définis dans le Code de la gouvernance et de la donnée créé par le Projet. Il se réfère par ailleurs à l'ordonnance du 8 mai 2014 *portant création et organisation d'un intégrateur de services régional* que le Projet abroge. Et il ne s'inscrit pas complètement dans les articles C.IV.15 et C.IV.16 du Projet (concernant la désignation des sources authentiques)[177]. **L'Autorité émet par conséquent d'entrée une réserve à propos de la cohérence de l'approche suivie par le Projet qui d'un côté, régit dans un Code approfondi, la gouvernance de la donnée, et de l'autre, met déjà en place une source authentique de données sous l'empire, inévitablement, d'un autre régime juridique *sui generis***.

188. L'Autorité conçoit cependant bien qu'il soit impossible d'organiser à ce stade, la désignation d'une source authentique en conformité intégrale au Code, dès lors que les divers avis requis par exemple, ne pourraient être recueillis, les institutions concernées n'existant pas encore. Toutefois, ceci n'empêche pas le demandeur de se référer aux concepts consacrés dans le Code d'une part, et d'autre part, l'Autorité l'inviterait à attendre que le Code soit mis en œuvre pour procéder à la désignation d'UrbIS comme source authentique de données. S'agissant d'une source authentique bruxelloise majeure, il semblerait regrettable qu'elle ne puisse bénéficier du cadre normatif fixé par le Code. Autrement dit, **l'Autorité recommande que la désignation d'UrbIS comme source authentique de données soit envisagées après l'adoption et l'entrée en vigueur du Code**.

189. Pour le reste, **s'agissant du traitement de données à caractère personnel**, l'Autorité **réitère son commentaire au sujet du concept de banque/base de données issues de sources authentiques qu'il convient d'abandonner**[178]. Il convient en conséquence d'identifier dans le Titre

[177] Par exemple, le Titre III recourt au concept « *d'initiateur* » de données, étranger au Code en projet, le Comité UrbIS peut ajouter de nouvelles données à la liste détaillée des données faisant partie du produit Brussels UrbIS alors que le Code prévoit à juste titre que c'est l'acte de désignation qui doit reprendre la liste des données contenues dans la source authentique

[178] Voir les considérants nos 65-71.

Au considérant n° 9 de son avis n° 001/2019 du 12 avril 2019 concernant un avant-projet d'arrêté de la Région de Bruxelles-Capitale en exécution de l'ordonnance du 8 mai 2014 *portant création et organisation d'un intégrateur de services régional et visant à désigner la banque de données cartographiques à grande échelle Brussels Urbis comme une source authentique régionale*, la Commission de contrôle bruxelloise « *s'interroge néanmoins sur le fait qu'UrbIS semble être une banque de données issue de sources authentiques et non une simple source authentique* », sans toutefois plus de précisions. L'Autorité observe qu'initialement, le demandeur d'avis auprès de la Commission de contrôle visait bien la mise en œuvre d'une source authentique de données.

III du Projet, conformément aux principes de prévisibilité et de légalité rappelés précédemment, les **éléments essentiels des traitements de données liés à la source authentique que le Projet entend mettre en œuvre**.

190. Le Chapitre 3 du Titre III du Projet, intitulé « *Les finalités poursuivies par Brussels UrbIS en tant que base de données issues de sources authentiques* », comprend un article 5 rédigé comme suit :

> « *Brussels UrbIS en tant que banque de données issues de sources authentiques, est le référentiel cartographique de base en Région de Bruxelles-Capitale, permettant de :*
> - *Superposer des informations géographiques entre elles ;*
> - *Connaître les coordonnées géographiques de n'importe quel lieu, qu'il s'agisse d'un point précis ou de n'importe quel objet géographique situés sur le territoire de la Région ;*
> - *Numériser des données métiers et les localiser sur un même référentiel ;*
> - *Échanger des données pouvant être reliées à Brussels UrbIS ;*
> - *Réduire les charges administratives dans le cadre du présent titre* » (souligné par l'Autorité)[179].

191. L'Autorité observe que **cette disposition identifie des traitements de données et non les finalités de ces traitements de données**[180]. S'agissant de la mise en œuvre d'une source authentique de données, le texte du rang de loi organisant cette source authentique doit notamment et avant tout, déterminer à quelle(s) fin(s) sont collectées les (catégories de) données à caractère personnel concernées, ces finalités étant indissociablement liées à la mission d'intérêt public en vue de laquelle la collecte des données est initialement réalisée par le responsable du traitement de la source authentique de données[181].

L'Autorité observe que le Conseil d'Etat n'a pas rendu d'avis au sujet du projet d'arrêté qui était alors soumis à la Commission de contrôle bruxelloise, voir http://www.raadvst-consetat.be/dbx/avis/65845.pdf#search=URBIS, dernièrement consulté le 06/10/2023.

[179] L'exposé des motifs se borne à répéter que « *Cette disposition indique les finalités poursuivies par la banque de données Brussels UrbIS dans la collecte des données qu'elle traite* ».

[180] Aux considérants nos 11-12 de son avis, cité à la note de bas de page n° 178, la Commission de contrôle bruxelloise avait cependant considéré ce qui suit :

« *L'article 5 de l'avant-projet d'*[arrêté] *décrit les finalités poursuivies par Brussels UrbIS en tant que source authentique.*

Ainsi, « Brussels UrbIS en tant que source authentique, a pour vocation d'être le référentiel cartographique de base en Région de Bruxelles-Capitale, permettant de :

-superposer des informations géographiques de n'importe quel point du territoire de la Région ;

-numériser des données métiers et les localiser sur un même référentiel ;

-échanger des données entre partenaires ».

Au vu et dans les limites de ce qui précède, la Commission estime que ces finalités sont déterminées, explicites et légitimes au sens de l'article 5, §1, b) du RGPD ».

L'article 4, 2), du RGPD définit le traitement de données comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

[181] L'exposé des motifs du Code reconnaît lui-même et correctement, cette logique :

192. Pour le reste, l'Autorité répète que l'ordonnance et le décret conjoints **doivent fixer l'ensemble des éléments essentiels** des traitements liés à la source authentique de données, conformément aux principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution, comme le Code en projet le rappelle d'ailleurs. L'Autorité relève en passant qu'une entité du type du Comité Brussels UrbIS visé à l'article 11 du Titre III du Projet ne dispose pas d'un pouvoir normatif et ne peut pas être compétente pour déterminer les éléments essentiels des traitements de données réalisés sur la base de la source authentique de données.

193. **Dans ces conditions, l'Autorité n'est par conséquent pas en mesure de poursuivre son analyse (qu'elle réserve) au sujet de la reconnaissance d'UrbIS comme source authentique de données**.

II.12. CONCLUSION

Par ces motifs,
L'Autorité est d'avis que

1. Bien qu'audacieux et novateur à certains égards, le Projet, qui entraîne une ingérence importante dans les droits et libertés des personnes concernées, soulève une préoccupation générale et importante sur le plan de la protection des données pour les trois motifs suivants : le dispositif du Projet tend à faciliter significativement le traitement des données par les autorités publiques bruxelloises et en particulier, la circulation des données entre ces autorités, notamment en poursuivant une dynamique de concentration dans le domaine du traitement de données ; il place une autorité publique incontournable, au cœur du traitement de données dans la Région de Bruxelles-Capitale ; sur le plan conceptuel, il semble porter une certaine conception patrimoniale de la donnée (à caractère personnel ou non) dont les conséquences concrètes sont floues (**considérants nos 4-22**) ;

2. La nécessité et la proportionnalité de la facilitation du traitement des données à caractère personnel par les autorités publiques bruxelloises doit être démontrée, et les garanties contre les risques pour les droits et libertés des personnes concernées doivent être déterminées et mises en évidence, à l'occasion d'une analyse d'impact (**considérants nos 15 et 27**) ;

« *Quand une Autorité publique crée et/ou gère une base de données, elle le fait conformément à une base légale qui lui assigne cette mission et dans le respect des principes applicables, notamment en matière de vie privée. Le mécanisme ici créé intervient dans un second temps : lorsqu'une base de données existe au sein d'une Autorité publique, elle peut être désignée pour servir de base de données de référence, en tant que source authentique, pour tout ou partie des données qui y sont incluses, pour d'autres Autorités publiques* ».

3. La nécessité et la proportionnalité de l'attribution de toutes ses compétences et pouvoirs au CIRB (PARADIGM) seul, doit être démontrée et les garanties contre les risques les risques pour les droits et libertés des personnes concernées doivent être déterminées et mises en évidence, à l'occasion d'une analyse d'impact (**considérants nos 19-27**) ;

4. La valorisation des données ne constitue pas en elle-même, une finalité déterminée de traitement de données à caractère personnel. Il convient d'identifier clairement l'impact de l'objectif de valorisation des données sur le traitement des données à caractère personnel, en identifiant son apport sur le plan juridique, les risques qu'il entraîne pour les droits et libertés des personnes concernées ainsi que les mesures mises en œuvre afin de limiter ceux-ci, et ce, à l'occasion d'une analyse d'impact (**considérants nos 21-22 et 27**) ;

5. Une qu'une disposition générale devrait spécifier que le Projet est sans préjudice du RGPD et ne peut être lu comme limitant les droits des personnes concernées ou les obligations du responsable du traitement (**considérant n° 26**) ;

6. L'article B.I.16, § 3, du Projet doit être adapté afin de garantir que, sans préjudice d'une norme du rang de loi prévoyant un accès libre et inconditionné du grand public aux documents concernés, afin d'accéder à un document administratif contenant des données à caractère personnel, le demandeur doit justifier de la finalité (légitime, déterminée, etc.) de l'utilisation (du traitement) des données envisagé, ce qui peut dans certains cas équivaloir à exiger de lui qu'il justifie d'un intérêt légitime (**considérants nos 28-32**) ;

7. Dans le cadre de la publicité passive de l'administration, le responsable du traitement doit disposer de la marge de manœuvre suffisante pour déterminer, compte-tenu des mesures techniques et organisationnelles à mettre en œuvre en exécution du RGPD, le mode de communication de données à caractère personnel (**considérants nos 33-35**) ;

8. Le Projet doit déterminer clairement le régime juridique applicable au consentement des personnes concernées lorsqu'il prévoit la possibilité d'y recourir (**considérants nos 36-37** – accès aux informations environnementales ; **considérants nos 120-121** – publication des décisions de la CADADO ; **considérants nos 141 et 146-151** – article C.III.14, § 3, du Projet) ;

9. La suppression de données d'un ensemble de données ne donne pas toujours lieu à une anonymisation des données (**considérants nos 38-39**) ;

10. L'article B.I.4 du Projet doit être motivé et adapté conformément aux principes de légalité et de prévisibilité (**considérants nos 40-45**) ;

11. Les principes de partage administratif de données consacrés dans les articles C.IV.4 et C.II.3, § 1er, du Projet doivent être revus à l'aune des principes applicables à l'échange de données entre autorités publiques (**considérants nos 46-50**) ;

12. Concernant le recours aux sources authentiques de données, l'article C.II.3, § 2, al. 1er, du Projet doit être adapté conformément au principe de minimisation des données. Celui-ci n'a pas pour seul objectif que les autorités publiques n'organisent pas elles-mêmes la collecte des données (auprès de la personne concernée). Le principe de collecte unique ne dispense pas le législateur de réaliser une analyse de compatibilité conformément à l'article 6, 4., du RGPD. La portée de l'article C.IV.13 du Projet doit être clarifiée et l'Autorité réserve son analyse à son sujet. Une source authentique de données est soumise aux principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution lorsqu'elle est sollicitée dans le cadre d'un traitement de données à caractère personnel. Enfin, le Projet doit prévoir les critères de désignation des sources authentiques de données (**considérants nos 51-64** ;

13. Il convient d'abandonner le concept de base de données issues de sources authentiques (**considérants nos 65-71**) ;

14. Le Projet prévoyant la réutilisation des documents administratifs par défaut, le législateur devra à l'avenir s'interroger, dans le cadre de ses projets de traitement, sur l'éventuelle nécessité d'interdire la réutilisation (**considérants nos 74-75**) ;

15. Le Projet doit être clarifié et le cas échéant développé, quant au régime juridique applicable à la réutilisation des données à caractère personnel, en transposition de la Directive Réutilisation et en exécution du Règlement sur la Gouvernance des Données (**considérants nos 82-86** – réutilisation dans le cadre de la Directive Réutilisation ; **considérants nos 87-99** – concernant le Règlement sur la Gouvernance des Données) ;

16. L'article C.V.10, § 3, du Projet, concernant la publication des cas de réutilisation de données, doit être précisé (**considérants nos 100-106**) ;

17. En l'état du dispositif du Projet, l'altruisme en matière de données ne peut pas être mis en œuvre (**considérants nos 105-106**) ;

18. Le Projet n'a pas pour objectif de faire de la CADADO une autorité de protection des données (**considérants nos 107-108**) ;

19. La communication systématique de données visée aux articles B.II.19 et B.II.20 du Projet est disproportionnée (**considérants nos 109-111**) ;

20. L'avis de l'Autorité ne peut être demandé que dans les conditions fixées par la LCA (considérants nos **114-119**) ;

21. Le demandeur doit envisager l'éventuelle anonymisation des avis et propositions de la CADADO avant publication (**considérant n° 122**) ;

22. La portée juridique des règles de gouvernance de la donnée doit être sûre et l'article C.III.1 du Projet, concernant le champ d'application des obligations applicables en la matière, est incomplet (**considérants nos 123-125**) ;

23. Les autorités publiques doivent se conformer aux régimes juridiques applicables aux données (**considérants nos 126-127**) ;

24. Le Projet doit clarifier ce que constitue la « *réversibilité* » des données. Au sens perçu par l'Autorité, celle-ci ne pourrait plus être réalisable lorsque l'autorité publique concernée ne peut plus traiter les données à caractère personnel concernées. Par ailleurs, notamment, la conservation d'une donnée dans son (ou ses) état(s) antérieur(s) ou sa remise dans un état antérieur constituent des traitements de données à caractère personnel qui doivent être justifiés conformément au RGPD (et au cadre normatif bruxellois ou autre, applicable) (**considérants nos 128-131**) ;

25. Les catégories de données visées à l'article C.III.10, § 1er, du Projet ne sont pas exclusives les unes des autres (**considérants nos 132-134**) ;

26. L'Autorité réserve son analyse sur la question de la valorisation des données d'usage, la disposition en projet nécessitant d'être approfondie (**considérants nos 135-140**) ;

27. L'article C.III.14, § 3, du Projet doit être clarifié et précisé (**considérants nos 141-152**) ;

28. L'article C.III.14, § 4, du Projet doit préciser qu'il n'est pas applicable aux plaintes concernant le traitement de données à caractère personnel, conformément à l'exposé des motifs du Projet. Par ailleurs, il doit être adapté à l'aune des principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution et le cas échéant, selon la position qui sera exprimée à son sujet par le Conseil d'Etat (**considérants nos 153-158**) ;

29. L'article C.III.16, als 3 et 4 ne peut en lui-même fonder une collecte de données à caractère personnel et doit être applicable dans les limites permises par les règles régissant la mission d'intérêt public ou l'obligation légale servant de fondement au traitement de données concernés (**considérants nos 159-161**) ;

30. L'Autorité réserve son analyse à propos de la distribution des données de référence visée à l'article C.III.17. Le responsable du traitement devrait être renseigné dans les métadonnées (**considérants nos 162-163**) ;

31. L'article C.III.18 du Projet ne pourra pas servir de fondement juridique à la prise de décisions automatisées à l'égard de personne concernées. Cette disposition contribue par ailleurs à la mise en œuvre de mesures pour la sauvegarde des droits et libertés des personnes concernées qui devront encore spécifiquement être prévues dans les textes normatifs dérogeant à l'article 22, 1., du RGPD (**considérants nos 164-166**) ;

32. Le Projet doit procéder à une meilleure identification des responsabilités au regard du traitement de données à caractère personnel dans son contexte (**considérants nos 167-172**) ;

33. En l'état du dispositif du Projet, l'article C.V.11 ne permettra pas de traiter des données à caractère personnel via le Centre d'exploitation et d'analyse des données. L'Autorité réserve par conséquent son analyse sur ce point (**considérants nos 173-174**) ;

34. L'article C.V.4 du Projet et son exposé des motifs doivent être approfondis à la fois en ce qu'il prévoit des traitements ultérieurs de données et en ce qu'il détermine la durée de conservation des données. L'Autorité réserve son analyse à ce sujet (**considérants nos 174-186**). Dans le cadre du Projet, la garantie selon laquelle les données doivent être détruites au terme d'un délai fixe est importante (**considérant n° 181**) ;

35. L'Autorité réserve son analyse quant à la désignation d'UrbIS comme source authentique de données, notamment dans un cadre distinct de celui prévu par le Code consacré dans le Projet (considérants nos **187-193**).

Pour le Centre de Connaissances,
(sé) Cédrine Morlière, Directrice