Numérisation de l'Etat– Quel contrôle sur les traitements de données des citoyens ?

25/04/2024

Florian Jacques

Assistant-doctorant à la Faculté de droit de l'Unamur et chercheur au Nadi/Crids

Plan de l'exposé

1. Introduction et mise en contexte
2. Un contrôle *a priori* – l'encadrement d'un traitement de données par les autorités publiques *via* les balises constitutionnelles
3. Le contrôle du citoyen sur les traitements de données à son sujet
4. Le contrôle exercé par l'intégrateur de services
5. Le contrôle des échanges de données réalisés *via* l'intégrateur de services
6. Réflexions sur la modification du règlement eIDAS – enjeu(x) et opportunité(s)

1. Introduction et mise en contexte

Rappel – principe du « Once Only » en CF/RW

- Textes principaux du cadre le légal :
  - Accord de coopération du 23 mai 2013 entre la RW et la CF portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative (A.coop. du 23 mai 2013)
  - Accord de coopération entre la RW et la CF du 15 mai 2014 portant exécution de l'accord de coopération du 23 mai 2013 […] (A.coop. du 15 mai 2014)

- Possibilité de désignation d'une base de données existante au sein d'une autorité publique (AP) comme source authentique de données (SA) (art. 7 A.coop du 23 mai 2013)
  - = « base de données […] contenant les données relatives à des personnes physiques ou morales, qui ont une **valeur unique pour les autorités publiques car leur collecte, stockage, mise à jour et destruction sont assurés exclusivement par une autorité publique déterminée**, appelée gestionnaire de source authentique, et qui **sont destinées à être réutilisées par les autorités publiques** » (art. 2, 1°A.coop du 23 mai 2013)

1. Introduction et mise en contexte

Rappel – principe du « Once Only » en CF/RW

- « Once Only » = principe de **collecte unique**

  - Obligation pour les autorités publiques (AP) de consulter les données à caractère personnel dans une SA de données si une SA existe :

Art. 11, A.coop. du 23 mai 2013

- Interdiction de (re)demander la donnée auprès **du citoyen ;**
- Interdiction de (re)demander la donnée à une **autre AP** ;
- Obligation de **préremplir** les formulaires ; et

Art. 6, A.coop. du 23 mai 2013

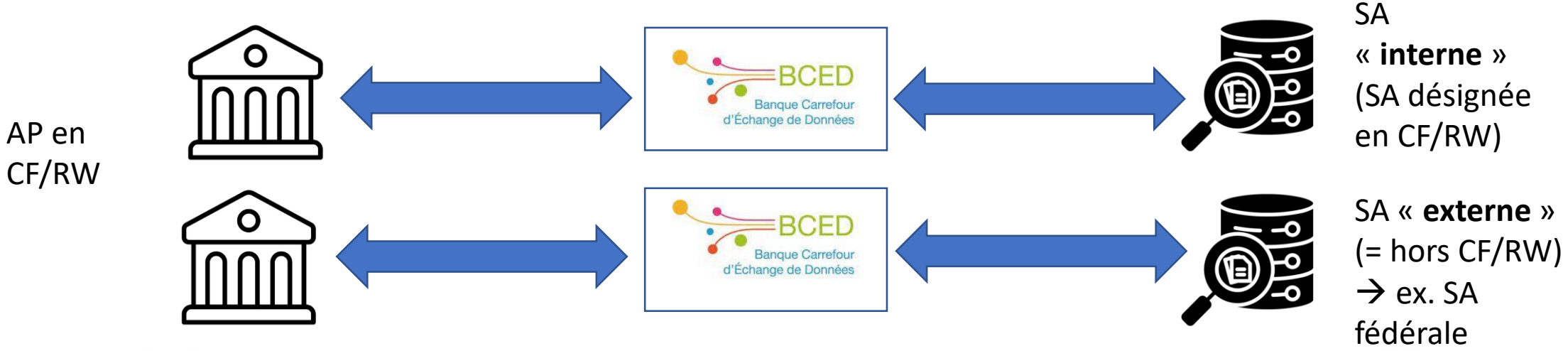
- Obligation d'accéder à la donnée issue de SA *via* l'intégrateur de service (cf. slide suivant)
  → (~~collecte directe auprès du gestionnaire~~)

- Simplification administrative pour le citoyen + évite la multiplication des copies de données.
- Multiplication des cas de **collecte indirecte** de données (auprès d'un tiers et non auprès du citoyen) + augmentation des cas de **réutilisation pour des finalités différentes** de celles pour lesquelles les données ont été initialement collectées.

1. Introduction et mise en contexte

L'intégrateur de services pour concrétiser ce principe

- Banque carrefour d'échange de données (BCED) désignée comme « intégrateur de services » (art. 2, 3°, A.coop du 23 mai 2013)
  - = une « institution légalement reconnue dont le **rôle principal** est d'**organiser** et de **faciliter l'échange de données** issues **de sources authentiques** […] **entre les différentes autorités publiques et autorités fédérales**, ainsi que **d'offrir des services d'accès hautement sécurisés aux sources authentiques**, dans le respect des prescrits de la vie privée » (art. 2, 3°,b), A.coop du 23 mai 2013).
  - Arts. 6 et 12 de l'accord de coopération du 23 mai 2013 → rôle central de la BCED



2. Un contrôle *a priori* – l'encadrement d'un traitement de données par les autorités publiques *via* les balises constitutionnelles

Plan :

a) L'exigence de légalité formelle
b) L'exigence de légalité matérielle/substantielle
c) En pratique – conséquence pour les échanges de données en RW et CF
d) La vérification de ces principes par l'APD *via* l'exigence de licéité du traitement

2. a) L'exigence de légalité formelle

Art. 22 de la Constitution → droit au respect de la **vie privé** « sauf dans les cas et conditions fixés par **la loi** »

- Garantie que toute atteinte à ce droit – et donc toute instauration d'un traitement de données à caractère personnel – soit organisée par **une loi au sens formel du terme**.

- → réserve de compétence au pouvoir législatif (garantie d'un débat parlementaire préalable)
  - Législateur décrétal en RW/CF.

- → ~~instauration d'un traitement de données à caractère personnel au moyen d'une norme de valeur règlementaire~~

- **Délégation possible au pouvoir exécutif** moyennant **détermination préalable des « éléments essentiels » du traitement** de données par une **norme de valeur législative**
  - Assouplissement de ce principe dans les cadre du « once only » → Cf. suite de l'exposé

2. b) L'exigence de légalité matérielle/substantielle

Exigence de **légalité matérielle** tend à assurer la **qualité**, la **clarté** et **prévisibilité** de la norme afin de permettre au citoyen de déterminer précisément à quelles conditions et dans quelles circonstances les autorités publiques peuvent s'ingérer dans son droit à la protection de la vie privée. Voy. notamment C.C., 15 mars 2018, n°29/2018 et C.C., 16 mai 2013, n° 66/2013, B.11.1.

- Obligation dans le chef du législateur de **déterminer les « éléments essentiels »** du traitement de données
  1. Finalité(s) du/des traitement(s) de données;
  2. Catégories de données à caractère personnel;
  3. Catégories de personnes concernées;
  4. Destinataires éventuels des données;
  5. Durée de conservation des données

Critères dégagés de la jurisprudence de la **Cour constitutionnelle**

→ Approche consacrée dans la légisprudence du **SLCE** (ex. avis n°69.730/VR)
→ Importance générale de **précision** des éléments essentiels (ex. SLCE,avis n.68.844/VR)

- APD considère également le responsable du traitement comme un élément essentiel du traitement
  - Principal **débiteur des obligations en matière de protection des données** consacrées dans le RGPD

2. b) L'exigence de légalité matérielle/substantielle

Finalité du traitement de données (= le « pourquoi ?» du traitement de données)

- Art. 5, §1er , b) du RGPD → exigence de traitement pour des finalités **<u>déterminées, explicites</u>** et légitimes
  - Exigence de clarté et de précision.

- → la finalité diffère de « l'opération de traitement réalisée »
- → la finalité diffère du « but d'intérêt général poursuivi par la norme »

Ex. APD, avis 226/2022, pp.5-6

- → la finalité doit être une « fin en soi, et non un moyen d'atteindre cette fin »

Voy. CPVP

- La **réutilisation de données à d'autres fins** nécessite une **nouvelle intervention du législateur**
  - → **Impossibilité de « présumer compatible » pour toutes réutilisations futures** ou « réputer compatibles des traitements ultérieurs » *via* une loi

Ex. APD, avis 65/2019 et 24/2021

2. b) L'exigence de légalité matérielle/substantielle

catégories de données à caractère personnel (= « sur quoi » porte le traitement de données ?)

- Concrétisation du « principe de **minimisation** »
  - → données doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées […] » (art. 5, §1er , c) du RGPD)
- **Détermination exhaustive** des catégories de données qui font l'objet du traitement dans la norme (~~recours aux listes exemplatives dans la norme~~). } Ex. APD, avis 64/2020
- Tension entre principe de **minimisation** et principe d'**exactitude**
  - → données doivent être « exactes et, si nécessaire, tenues à jour […] rectifiées sans tarder » (art. 5, §1er, d) du RGPD)
  - → Dans le cadre d'une SA, l'exigence d'exactitude peut primer sur la minimisation (voy. APD, Avis 143/2023 → identification des personnes au moyen du numéro de RN dans la SA)

- **Catégories de personnes** (= « qui » est visé par le traitement de données à caractère personnel ?).

2. b) L'exigence de légalité matérielle/substantielle

Destinataires des données (= « quelles autres entités » peuvent accéder aux données ?)

- Importance de **déterminer avec suffisamment de précision les destinataires de données**
  - Cf. C.C., 22 septembre 2022, n°110/2022
    - Texte prévoyant que les données peuvent être transmises à des tiers
    - + délégation au CSI du pouvoir de déterminer ces tiers

Annulation au motif de **non détermination d'un élément essentiel du traitement** (catégories de destinataires)

- Lien avec la finalité du traitement
  - → une fois l'objectif clairement défini il devient possible de savoir « qui » doit accéder aux données pour atteindre cet objectif.

2. b) L'exigence de légalité matérielle/substantielle

Durée du traitement (= « pendant combien de temps » les données sont traitées ?)

- Concrétisation du principe de limitation de la conservation
  - Données doivent être conservées « pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées […] » (art. 5, §1er , e) du RGPD).
  - → pas de conservation *ad vitam aeternam*

- Fixation d'un délai maximum ou de critères utilisés pour déterminer la durée de conservation (ex. art. 13, 14 et 15 du RGPD qui consacrent ce principe)

  - Si fixation d'un délai max. → doit être adapté par rapport à la finalité de traitement
    - Une durée de conservation relativement courte peut être « trop longue »

  - Si fixation de critères pour déterminer la durée de conservation → éviter les mécanismes qui présentent un risque inhérent de conservation sans limite des données à caractère personnel
    - Ex. SLCE, Avis 72.597/VR du 20 janvier 2023

- Absence de détermination par le législateur est un motif d'annulation (ex. C.C., 22 septembre 2022 n°110/2022).

2. c) En pratique – conséquence pour les échanges de données en RW et CF

Nécessité d'intervention normative en vue de permettre l'échange de données

Intervention du **législateur décrétal** pour la **création d'une base de données** (= instauration d'un traitement de données) → principe de légalité formelle

Intervention du **législateur décrétal** pour **le traitement de données ultérieur** (=instauration d'un nouveau traitement de données) afin de **permettre l'accès aux données (contenues dans une SA)** de données → art. 6.4 du RGPD et principe de légalité formelle

→ légalité matérielle en déterminant la finalité constitue le fondement de la possibilité d'accès aux données (contenues dans la SA).

Intervention du **législateur décrétal ou du pouvoir exécutif** (arrêté du gouvernement) pour la désignation d'une base de donnée préexistante comme SA (>< BDSA uniquement par décret)

→ **assouplissement à l'exigence de légalité formelle**

→ contenu de l'acte de désignation (art. 7, § 1er et §2 de l'accord de coopération du 23 mai 2013)

→ voy. toutefois APD avis 65/2019 :

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

2. d) La vérification de ces principes par l'APD via l'exigence de licéité du traitement

Art. 5, §1er , a) et 6 du RGPD → **exigence de licéité du traitement**

→ Chaque traitement de données doit avoir une base de licéité

→ Liste exhaustive et limitative des bases de licéité inscrites à l'article 6 du RGPD

→ Traitements de données réalisés par une autorité publique se fondent, généralement, sur l'une des deux hypothèses suivantes :

1. « Le traitement [qui] est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis » (art. 6, §1er c) du RGPD) ; ou
2. « Le traitement [qui] 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 » (art. 6, §1er e) du RGPD).

2. d), i) – Obligation légale (art. 6.1.c))

Conditions d'application de la base de licéité

- La norme doit être **en vigueur** (décision 143/2021)
- La norme doit être **contraignante** en droit national (décision 47/2022)
- La norme doit contenir une réelle **obligation** de traitement, par opposition à une simple autorisation (décision 34/2022)
- **Nécessité** du traitement
  - Principe de **minimisation** (décisions 38/2021, 162/2022)

Conditions de qualité de la norme

Arts. 7 et 8 de la Charte

- Clarté, prévisibilité et précision
- Besoin social impérieux

→ - « ancrage normatif large » (décision 55/2021)
- plusieurs opérations de traitement pour une même base légale (décision 162/2022

Art. 22 Const.

- Légalité matérielle
- Légalité formelle

Art. 6.3 RGPD

- Conditions générales de licéité du traitement
- Contenu et prévisibilité (pas de marge d'appréciation injustifiée)

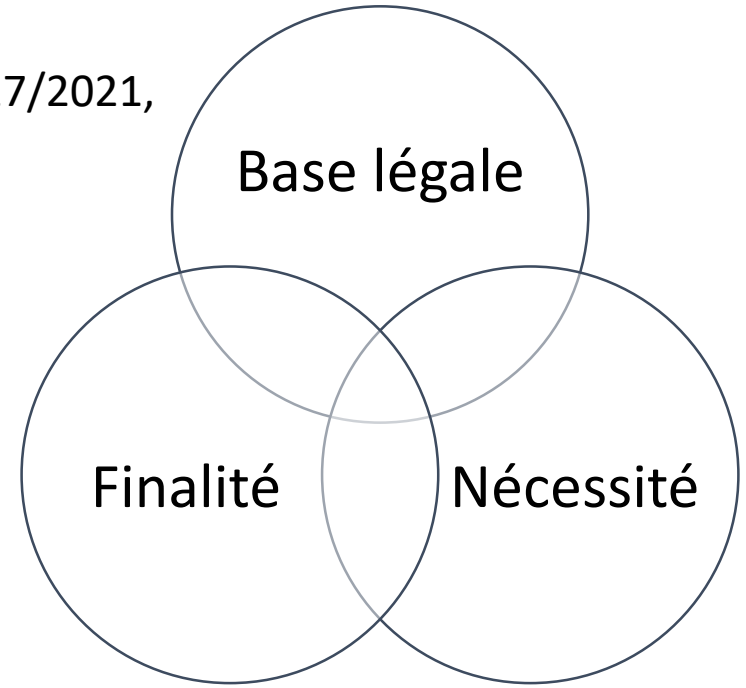
2., d), ii) – Mission d'intérêt public (art. 6.1.e))

Conditions d'application de la base de licéité

- Une **base légale** doit contenir la mission d'intérêt public du responsable du traitement (Article 8 de la Charte et ingérence prévue par la loi)
  - Exigences de qualité de la norme (Arts. 7 et 8 de la Charte, art. 22 Constitution et art. 6.3 du RGPD) => caractéristiques essentielles du traitement

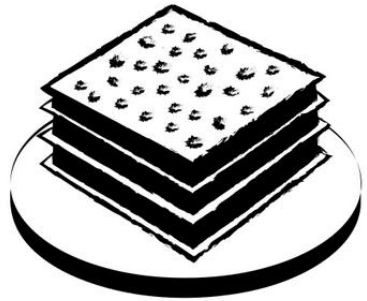
  - Mais les missions d'intérêts publics ne sont pas nécessairement circonscrites avec précision
    - **Habilitation générale** à traiter les données : « nécessaires à l'exécution de la mission » (décisions 124/2021, 149/2022)
    - Ne peut se dispenser du principe de finalité (décisions 55/2021, 127/2021, 71/2022, 100/2022, 149/2022)

- **Nécessité et minimisation** du traitement
  - Pondération *in concreto* par le responsable du traitement (décisions 124/2021, 149/2022)



3. Le contrôle du citoyen sur les traitements de données à son sujet

Plusieurs « couches » de mécanismes de contrôle

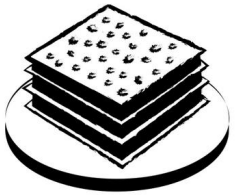


1. Mécanismes de contrôle inscrits **dans le RGPD**

UNION EUROPÉENNE

2. Mécanismes de contrôle **<u>supplémentaires</u>** inscrits dans les **accords de coopération en matière d'échange de données**

3. Le contrôle du citoyen sur les traitements de données à son sujet

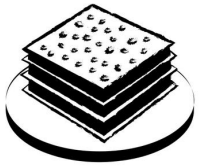


1. Mécanismes de contrôle inscrits dans le RGPD

UNION EUROPÉENNE

- Principes applicables aux traitements et exigence de licéité
- Transparence érigée en principe applicable a tous traitements;
- Exigence d'intervention du législateur pour la réutilisation (dans le secteur public);
- Droits de la personnes concernée (droit à l'information, droit d'accès, droit de rectification, droit à l'effacement, droit de s'opposer à un traitement, …);
- Droit de s'adresser à une autorité de contrôle;
- ….

3. Le contrôle du citoyen sur les traitements de données à son sujet



Mécanismes de contrôle supplémentaires inscrits dans les accords de coopération en matière d'échange de données

- « **Once only** » comme mécanisme de contrôle
- Tenue, par la BCED, d'un **référentiel des données** disponibles et d'un **annuaire des SA**;
- Tenue par la BCED, d'un **cadastre des flux** entrant et sortant des SA rendu accessible au public;

Art. 11, A.coop. du 23 mai 2013

- Droit pour toutes personne de « **connaitre toutes les autorités publiques qui ont, au cours des six mois écoulés, consulté ou mis à jour ses données** »;

Art. 17, A.coop. du 23 mai 2013

- Tenue d'un **registre nominatif** des personnes autorisées à accéder aux données pour les AP qui ont accès aux SA;

Art. 12, A.coop. du 23 mai 2013

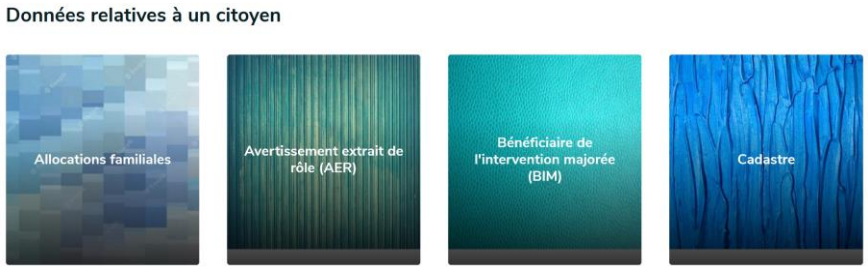
- (autorisation préalablement au traitement de données de SA)

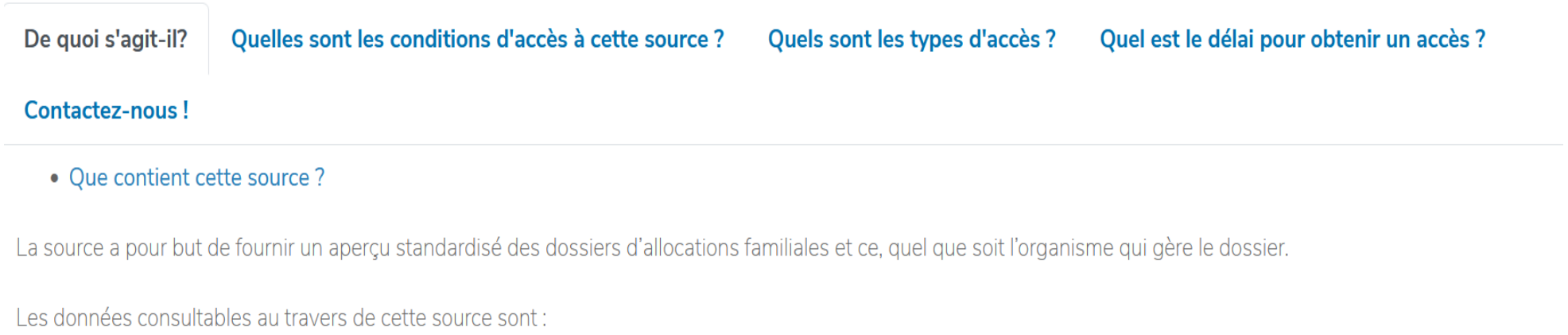
Art. 24, A.coop. du 23 mai 2013

- **Nature** de ces mécanismes → Cf. APD avis 65/2019 exigences de transparence additionnelles saluées mais rappel qu'elles sont sans préjudice des droits consacrés dans le RGPD.

3. Le contrôle du citoyen sur les traitements de données à son sujet

Mécanismes de contrôle supplémentaires inscrits dans les accords de coopération en matière d'échange de données





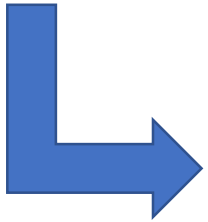
- *Quid* en pratique ?

4. Le contrôle exercé par l'intégrateur de services

Banque Carrefour d'Échange de Données
L'intégrateur de services pour la Région wallonne et la Fédération Wallonie-Bruxelles

Intervention de la BCED dans le cadre du **processus de désignation d'une SA**

- Réalisation d'une **analyse d'opportunité**



Art. 5. A.coop du 15 mai 2014

  - Intervention ***a priori*** (formalité préalable)
  - Limité au cas de **désignation d'une SA par arrêté d'un gouvernement** (>< ~~décret~~)
  - **Champ** de l'analyse → comprend, notamment, les exigences en matière de protection des données à caractère personnel
  - **Objectif** = vérification que la « BD candidate » présente les garanties suffisantes pour être désignée comme SA
    - Accompagnement dans le processus de reconnaissance;
    - Suspension du projet;
    - Abandon du projet

4. Le contrôle exercé par l'intégrateur de services

Intervention de la BCED dans le cadre du **processus de désignation d'une SA**

- Réalisation d'une **analyse d'opportunité**
  - **Importance accordée à cette formalité par la SLCE** (ex. avis n°73.086/2 et 68.476/4)

> 23 mai 2013 [2]. Par ailleurs, il est également requis que préalablement à l'adoption de cet arrêté, la Banque-Carrefour d'échange de données (ci-après « BCDE ») prévue à l'article 2, 3°, du même accord de coopération, ait effectué l'analyse visée à l'article 5, §§ 2 et 3, de l'accord de coopération du 15 mai 2014.
>
> Les exigences liées à l'accomplissement de ces formalités revêtent, dans la procédure d'adoption de l'arrêté et donc dans l'exercice, par le Gouvernement, de l'habilitation qui lui est conférée, un caractère particulièrement déterminant.
>
> Il appartient donc à l'auteur du projet de procéder à l'accomplissement de ces formalités et d'en faire mention au préambule [3].

  - Conséquences en cas de non-réalisation de la formalité ?

  - **Nature de la décision** d'abandon/d'accompagnement à l'issue de l'analyse d'opportunité ?
    - Limites à ne pas franchir (cf. jurisprudence CSI dans la suite de l'exposé)
      - Différence toutefois = décision de désignation revient au pouvoir exécutif

4. Le contrôle exercé par l'intégrateur de services

Intervention de la BCED dans le cadre du **processus de désignation d'une SA**

- Rappel de l'APD → avis 143/2023 du 29 septembre 2023

II.3. Procédure de « *labellisation* »

34. L'article 5 du Projet fixe une procédure de « *labellisation* » au terme de laquelle **la BCED peut attribuer le statut de source authentique de données** à une base de données répondant aux conditions fixées dans l'article 5, § 1er. L'article 6 du Projet création BCED précise que c'est le responsable de de la BCED[26] qui est compétent pour attribuer à une source son statut de source

36. **L'Autorité est d'avis que le Projet doit à tout le moins prévoir qu'un arrêté du Gouvernement doit être adopté pour qualifier une banque de donnée de source authentique de données**. En effet, la qualité de source authentique qui est attribuée à une banque de données constitue clairement un élément essentiel des traitements de données mis en place (elle relève de la finalité du traitement) : c'est de cette qualité que découle le mode indirect (et obligatoire) de collecte des données auprès de la source concernée, via la BCED, en exécution du Projet. Ce n'est par conséquent que compte-tenu des spécificités du Projet et de sa logique (à savoir la mise en place d'un dispositif général organisant le recours systématique aux sources authentiques de données) que l'Autorité a accepté antérieurement que le statut de source authentique puisse être attribué par une norme réglementaire (et non directement par une norme du rang de loi), sans pour autant méconnaître les principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution[27].

Déléguer ce pouvoir à une autorité publique telle que la BCED (*in concreto*, à son responsable) méconnaît ces principes.

5. Le contrôle des échanges de données réalisés *via* l'intégrateur de services

Solutions envisageables comprennent

1. Le contrôle par une **autorité *Ad hoc*** indépendante notamment de l'intégrateur de services
   - ***Ex.*** Commission de contrôle bruxelloise (ordonnance du 8 mai 2014 portant création et organisation de l'intégrateur de service régional)
2. Le contrôle par **l'Autorité de protection des données (APD)**

APD Autorité de protection des données

GBA Gegevensbeschermingsautoriteit

5. Le contrôle des échanges de données réalisés *via* l'intégrateur de services

1. Le contrôle par une **autorité *Ad hoc*** indépendante notamment de l'intégrateur de services

- Accord de coopération du 23 mai 2013 prévoit la mise en place d'une « Commission Wallonie-Bruxelles de contrôle des échanges de données » ou **« CCED »**. (arts. 22-30)
  - Indépendante de la BCED notamment
- Commission **jamais instaurée**
- **Vouée à ne jamais voir le jour ?**

A retenir

Tiers indépendant doté de compétences intéressantes
-avis obligatoire (BDSA – SA désignée par Arrêté du gouvernement) (art. 7)
-compétence d'autorisation avant traitement de données issues de SA (*via* BCED)

II.6. Suppression de la Commission Wallonie-Bruxelles de contrôle des échanges de données

54. **Le Projet supprime la Commission Wallonie-Bruxelles de contrôle des échanges de données (CCED)**[37]. Il apparaît en pratique que cette institution n'a jamais été instituée. Celle-ci et

APD, avis 143/2023

5. Le contrôle des échanges de données réalisés *via* l'intégrateur de services

1. Le contrôle par une **autorité *Ad hoc*** indépendante notamment de l'intégrateur de services

- Leçon pour le futur – contrôle par un tiers indépendant avec **compétences (1) d'avis et (2) d'autorisation**

- Compétence d'avis obligatoire a *priori* avant désignation de S.A – importance du respect de la formalité
  - Si **objet de l'avis est un arrêté**
  - Si **l'objet de l'avis est une norme de valeur législative**
    - Compétence de la Cour constitutionnelle pour contrôler le processus d'élaboration d'une norme « lorsque les règles qui contribuent à définir ce processus peuvent être considérées comme tendant à garantir les droits et libertés reconnus par le titre II […] de la Constitution » (C.C., 26 septembre 2019, n°121/2019, B.13.2. ;C.C., 16 février 2023, n°26/2023, B.30.1)
      - → 26/2023 → application du principe en l'absence de consultation de l'APD (VTC consultée)
      - → *contra* C.C., 17 mai 2023, n°75/2023 rejet du recours malgré absence de consultation de l'APD
        - Argument retenu = pas de modification du traitement de donnée existants
          - >< APD avis 143/2023 → désignation en tant que SA = élément essentiel du traitement (concerne la finalité).

5. Le contrôle des échanges de données réalisés *via* l'intégrateur de services

1. Le contrôle par une **autorité *Ad hoc*** indépendante notamment de l'intégrateur de services

- Leçon pour le futur – contrôle par un tiers indépendant avec compétences (1) d'avis et (2) d'autorisation

- Compétence d'autorisation
  - Compatibilité avec le RGPD
    - incompatibilité avec le RGPD (cf. art.1er , §3) ?
    - Possible en application de l'art. 6, §2 ? → mesures en vue de garantir « un traitement loyal et licite »
    - Art. 36, §5 du RGPD
  - **Limites** du pouvoir d'autorisation
    - Jurisprudence CSI → détermination des éléments essentiels du traitement interdite

C.C., 22 septembre 2022, n°110/2022
C.C., 1er juin 2021, n°84/2023

Art. 5 de l'accord de coopération « vaccination » et art. 10 de l'accord de coopération « *tracing* » → **délégation au CSI du pouvoir de déterminer des catégories de destinataires de données**

  - Importance du **respect de la formalité**
    - Mesures correctives adoptées par l'APD en cas de non-respect (ex. interdiction temporaire/définitive de traitement) ?
      - Illicéité du traitement qui ne respecte pas une mesure visant à garantir le traitement loyal et licite ?
      - Compétence de l'APD → contrôle de l'application du RGPD mais **aussi des « lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel […] »** (Art. 4, §1er de la loi du 3 décembre 2017).

5. Le contrôle des échanges de données réalisés *via* l'intégrateur de services

1. Le contrôle par une **autorité *Ad hoc*** indépendante notamment de l'intégrateur de services

- Leçon pour le futur – contrôle par un tiers indépendant avec compétences (1) d'avis et (2) d'autorisation
- Compétence <u>d'autorisation</u> – suite
    - **Nature** de l'autorisation → ne constitue pas une base de licéité, au sens du RGPD, à elle seule !
        - Jurisprudence de l'APD :
            - Décision 31/2022 : délibération d'un Comité sectoriel n'est **pas** une base de licéité en soi
            - Décision 127/2021 : compétence de l'APD vis-à-vis des législations contraires au RGPD (// EDPB)

L'APD pourrait écarter une délibération du CSI

5. Le contrôle des échanges de données réalisés *via* l'intégrateur de services

Le contrôle par **l'Autorité de protection des données (APD)**

- Question de la **compétence de l'APD vis-à-vis de l'intégrateur de services**

- BCED est-elle responsable de traitement conjointement avec la SA et l'AP qui accède aux données de la SA (*via* la BCED) en raison des mission d'intégrateur de service que la loi lui impose (APD, avis n°65/2019)

Compétence attribuée dans le texte soumis pour avis à l'APD ou obligation imposée aux AP/SA	Accords de coopération en vigueur
Développer **les normes, les standards et l'architecture de base nécessaire pour une mise en œuvre efficace** […] de la **stratégie commune** en matière de partage de données	Art. 11, §2, 4), A. coop du 23 mai 2013
Développer des **projets et services englobant potentiellement l'ensemble des autorités publiques** […]	Art. 11, §2, 5), A. coop du 23 mai 2013
Gérer la collaboration avec les autres autorités en matière de partage de données […]	Art. 11, §2, 7), A. coop du 23 mai 2013
Mettre en place les moyens techniques pour communiquer les informations entre elle et les sources authentiques […] , entre **elle et les autorités publiques** et entre elle et les destinataire	Art. 11, §2, 7), a), A. coop du 23 mai 2013
AP « utilisent la [BCED] pour accéder [aux SA] et aux [BD SA] ainsi qu'aux sources authentiques externes […]	Art. 12, §2, A. coop du 23 mai 2013
SA doivent autoriser la BCED à « consulter, copier et transmettre les données contenues dans lesdites sources ou banques »	Art. 12, §1er, A. coop du 23 mai 2013

- Quelle position de la BCED par rapport à cette approche ?

- Embrasser cette qualification pour avoir une **plus grande autonomie décisionnelle** vis-à-vis des traitements (échanges) de données réalisés *via* la BCED ?

6. Réflexions sur la modification de règlement eIDAS – enjeu(x) et opportunité(s)

Proposition de règlement […] en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique

- **Modification du règlement eIDAS** (règlement 910/2014)
- Texte adopté en première lecture par le Parlement européen le 29/02/2024
- Introduction du « **portefeuille européen d'identité numérique** »

  = **moyen d'identification électronique** permettant à son utilisateurs **d'utiliser des données d'identification personnelle**, le cas échéant **en combinaison avec des attestations électroniques d'attributs** , pour **s'authentifier auprès de parties utilisatrices** en vue de **l'usage transfrontalier de services publics** ou privés en ligne et hors ligne (arts. 1, 42) et 5bis, §4).

  - **Attestation électronique d'attribut** = une attestation sous forme électronique qui permet l'authentification d'une **caractéristique**, une **qualité,** un **droit** ou une autorisation d'une personne physique ou morale […]
  - Obligation pour les EM de **délivrer au moins un portefeuille** européen d'identité numérique

6. Réflexions sur la modification de règlement eIDAS – enjeu(x) et opportunité(s)

Proposition de règlement […] en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique

- **Enjeu** = introduction d'un **nouveau service de confiance** → service qualifié de fourniture « d'attestations électroniques d'attributs » → interfacé avec le portefeuille d'identité numérique

- Pour certains attributs (énumérés dans une nouvelle annexe VI du règlement)
  - Obligation pour les EM de **permettre aux prestataires** de services de confiance qualifiés **de vérifier** par des moyens électroniques, **à la demande de l'utilisateur**, l'authenticité des attributs, par rapport à une SA du secteur public (si SA existe au niveau national)

  - → obligation de permettre l'accès à des entités privées au SA ?

- **Opportunité** de contrôle dans le chef du citoyen (art. 5bis, §4 du règlement modifié)
  - Portefeuille doit offrir des **fonctionnalités visant à assurer le droit à la protection des données** parmi lesquelles l'accès à un journal des transactions effectuées au moyen du portefeuille permettant
    - Consultation **d'une liste à jour des parties utilisatrices avec lesquelles l'utilisateur a établi une connexion** et, le cas échéant, de toutes les **données échangées**; et
    - **Signalement à l'autorité de protection des données** lorsqu'une demande de données présumée illégale ou suspecte est reçue.

Merci de votre attention !

Des questions ?

Florian.jacques@unamur.be