Recommandation n° 09/2012 du 23 mai 2012

Concerne : recommandation d'initiative relative aux sources authentiques de données dans le secteur public (CO-AR-2010-005)

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

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 30 ;

Vu le rapport de madame F. D'Hautcourt et de monsieur F. Robben ;

Émet le 23 mai 2012 la recommandation suivante :

I. OBJET DE LA RECOMMANDATION

1. La jurisprudence de la Commission[1] et de ses comités sectoriels[2] renvoie souvent au principe de la "source authentique". Ce principe est lié à celui de la collecte unique de données. Tous deux visent une collecte unique de données auprès de citoyens et d'entreprises[3] pour ensuite stocker ces données dans des sources authentiques – gérées par des autorités publiques – et les rendre accessibles à d'autres instances (publiques). Le but est d'éviter qu'une autorité ne réclame une donnée à des citoyens / entreprises alors que cette information est déjà connue d'une autre instance publique.

2. Les sources authentiques occupent donc, avec les intégrateurs de services (cf. recommandation de la Commission n° 03/2009), une position cruciale dans le contexte de l'e-government belge, et cela transparaît aussi de plus en plus dans la réglementation en la matière[4].

3. La Commission estime que, vu leur position clé, les sources authentiques ont potentiellement un impact important sur la protection de la vie privée de chaque citoyen et que lors des traitements de données intervenant dans le cadre d'une source authentique, il convient donc de veiller à ce que la LVP soit rigoureusement respectée. L'application de la LVP à un concept relativement nouveau et abstrait tel que celui des sources authentiques ne va toutefois pas de soi. Dans cette optique, la Commission donne, par le biais de la présente recommandation, un certain nombre de directives dont les instances responsables de la création et de la gestion de sources authentiques dans le secteur public doivent en tout cas tenir compte. La Commission utilise dans ce contexte le critère fonctionnel[5] pour déterminer si une instance assure ou non un service public.

---

[1] Exemples : avis n° 42/2006, 01/2008, 36/2008, 11/2009, 14/2010, 14/2011, 16/2011, 18/2011 et 34/2011.

[2] Exemples : délibérations du Comité sectoriel pour l'Autorité Fédérale n° 03/2009, 05/2009, 06/2009, 13/2009, 16/2009, 01/2010 et 13/2011.

[3] Par souci d'exhaustivité, la Commission attire l'attention sur le fait qu'il existe également des sources authentiques contenant des informations créées par les pouvoirs publics eux-mêmes et qui ne sont donc pas réclamées auprès des citoyens/entreprises.

[4] À titre d'exemple :

- article 2, 2°, articles 3 et 4 du décret flamand du 18 juillet 2008 *relatif à l'échange électronique de données administratives* ;
- article 3, § 1er, (b), deuxième alinéa de l'accord de coopération du 28 septembre 2006 qui reconnaît le principe de la collecte unique et de la réutilisation maximale des données en utilisant des sources authentiques de données (Accord de coopération entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire française et la Commission communautaire commune *concernant les principes pour un e-gouvernement intégré et la construction, l'utilisation et la gestion de développements et de services d'un e-gouvernement intégré* (M.B. 19/10/2006).

[5] Cf. A. Mast, J. Dujardin, M. Van Damme, J. Vande Lanotte, *Overzicht van het Belgisch Administratief Recht*, Mechelen, Kluwer, 2006, point 66 : *"L'expression service public est utilisée dans deux significations : l'une vise l'organisme, l'autre la fonction. Dans la première signification, appelée la signification organique, on vise un organisme de droit public, comme par exemple l'Office national de Sécurité sociale, auquel une tâche d'intérêt général est confiée. Dans la deuxième signification, appelée la signification fonctionnelle, on ne se on se focalise que sur la tâche d'intérêt général ; ainsi, le concessionnaire, une personne privée, assure la gestion d'un service public.*" [Traduction libre réalisée par le Secrétariat de la Commission, en l'absence de traduction officielle].

II. CARACTÉRISTIQUES DES SOURCES AUTHENTIQUES

4. La Commission constate que certaines sources authentiques sont explicitement désignées dans la réglementation[6]. D'autres sources authentiques sont implicitement soutenues par la réglementation[7] ou sont généralement admises dans la pratique comme étant une source authentique (sans que cela découle explicitement ou implicitement de règles juridiques).

5. La Commission considère que les sources authentiques possèdent un certain nombre de caractéristiques communes :

    a. la source est la référence par excellence pour obtenir certaines données et elle offre des garanties spécifiques en termes d'exactitude, d'exhaustivité et de disponibilité de ces données ;
    b. les citoyens et les entreprises ne doivent en principe fournir ces données qu'à cette source (éventuellement via une autre instance qui se charge de la collecte et/ou de la validation des données (cf. ci-après aux points 6-8)) ;
    c. toutes les autres instances publiques réclament ces données auprès de cette source de sorte qu'elles ne doivent plus assurer chacune séparément la collecte des mêmes informations ; une source authentique remplit ainsi une fonction centrale pour plusieurs finalités.

III. TRAITEMENTS DE DONNÉES INTERVENANT DANS LE CADRE DES SOURCES AUTHENTIQUES – APPLICATION DE LA LVP

A. PRINCIPAUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE D'UNE SOURCE AUTHENTIQUE

---

[6] Cf. article 2, 2° du décret flamand du 18 juillet 2008 *relatif à l'échange électronique de données administratives* ; article 2, 5° *iuncto* article 29, § 2 de l'avant-projet de loi *relatif à l'institution et à l'organisation d'un intégrateur de services flamand* approuvé le 1er mars 2012 par le Conseil des Ministres.

[7] Loi du 8 août 1983 *organisant un registre national des personnes physiques*. La loi n'utilise pas le terme "source authentique" mais tout indique que le Registre national en est une.

Article 3 de la loi du 16 janvier 2003 *portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions* (M.B. du 5 février 2003) : "*Il est créé au sein du Service public fédéral Économie, P.M.E., Classes moyennes et Énergie un registre, dénommé "Banque-Carrefour des Entreprises". Ce registre associé à l'introduction du numéro unique d'entreprise a pour objectif, en application du principe de collecte unique de données, de permettre de simplifier les procédures administratives s'adressant aux entreprises ainsi que de contribuer à l'organisation plus efficace des services publics.*"

6. La Commission estime que dans le cadre d'une source authentique, on peut distinguer quatre grands groupes de traitements de données à caractère personnel (appelés ci-après "les 4 phases") :

    a. collecte ;

    b. validation ;

    c. gestion ;

    d. mise à disposition.

7. Dans certains cas, les processus précités sont exécutés par une seule et même instance ; dans d'autre cas, plusieurs acteurs interviennent. À titre d'exemple :

    a. pour le Registre national, les phases a et b sont assurées par les communes (registres de population) tandis que les phases c et d sont assurées par le Registre national ;

    b. pour les données de revenus qui sont introduites par le citoyen via la déclaration fiscale : les quatre phases sont assurées par le SPF Finances.

8. La Commission considère que sur ce plan, chaque projet présente des caractéristiques spécifiques et elle laisse les responsables du traitement établir quel modèle est le plus approprié dans une situation concrète[8]. Elle souligne uniquement que la LVP doit être respectée dans tous les cas, ce qui peut évidemment avoir des implications sur l'architecture de la source authentique[9].

B. POINTS IMPORTANTS DU POINT DE VUE DE LA LVP

1) Finalité

9. Du point de vue de la LVP, le fait que l'élaboration d'un système de sources authentiques distribuées permette d'éviter le stockage de grandes quantités de données dans une même "super banque de données" constitue indéniablement un point positif. Cela n'empêche pas qu'une zone de tension puisse apparaître entre, d'une part, la collecte unique et, d'autre part, l'article 4, § 1, 2° de la LVP aux termes duquel des données collectées pour des

[8] Sauf évidemment si le législateur a tout réglé en la matière. Par exemple : le Registre national est alimenté par les registres de population. La loi prévoit que ces derniers sont gérés par les communes ; le responsable du traitement ne peut donc pas décider de sa propre initiative de confier la gestion des registres de population aux provinces, par exemple.

[9] La directive reprise au point 18, b. de la présente recommandation en est une illustration : sa mise en œuvre peut avoir une influence sur l'architecture.

finalités déterminées, explicites[10] et légitimes ne peuvent pas être traitées ultérieurement *de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables*. La collecte unique ne peut pas avoir pour effet de passer outre l'article 4, § 1, 2° de la LVP.

10. La Commission précise toutefois que le principe de finalité n'implique pas nécessairement que dès la création de la source authentique, il faille donner une énumération exhaustive des finalités pour lesquelles des données seront utilisées dans le futur. Ce principe signifie par contre que si à un stade ultérieur, des traitements ont lieu pour de "nouvelles" finalités, il conviendra de toujours vérifier si ces finalités sont compatibles avec les finalités initiales et ce, comme déjà indiqué au point 9, en tenant compte de tous les facteurs pertinents.

11. Ce qui précède est d'ailleurs d'autant plus important que les comités sectoriels institués au sein de la Commission – dans le cadre de l'évaluation de demandes d'autorisation (cf. infra le point 27) – soumettront notamment la compatibilité des traitements ultérieurs de données à un examen approfondi.

12. Ces Comités peuvent d'ailleurs – pour autant que cela n'aille pas à l'encontre de dispositions réglementaires existantes – déclarer aussi eux-mêmes un traitement ultérieur comme étant compatible. Une autorisation constitue en effet une décision normative qui est rendue publique de sorte que de telles décisions peuvent être considérées comme une "disposition réglementaire" au sens de l'article 4, § 1, 2° de la LVP.

2) Proportionnalité

13. Dans le cadre d'une source authentique, il est uniquement permis de collecter/conserver/transmettre des données pertinentes et non excessives. En la matière, le principe de proportionnalité impose des restrictions à plusieurs niveaux, notamment en ce qui concerne :

    a. le groupe de personnes concernées au sujet desquelles des données sont traitées ;

    b. la nature et la quantité de données qui sont traitées ;

    c. les catégories de tiers auxquels les données peuvent être fournies.

14. La source authentique doit – éventuellement avec l'intervention d'un intégrateur de services encadré légalement à cet effet – garantir le respect du principe de proportionnalité.

[10] Il convient donc d'éviter de définir les finalités de façon générale ou trop vague.

15. En outre, les données doivent être recueillies autant que possible au moyen d'une collecte unique. Dès lors, il convient en principe d'éviter que plusieurs organisations publiques conservent toutes sortes de fichiers avec des copies des mêmes données. Si c'est quand même nécessaire pour créer des fichiers dérivés, il faut en tout cas garantir que ces fichiers seront régulièrement mis à jour au moyen des données de la source authentique. En outre, les fichiers dérivés doivent toujours offrir des garanties similaires en matière de sécurité que la source authentique elle-même.

16. La Commission est néanmoins consciente que la recherche d'une "unicité" (une donnée, une source authentique) peut également entraîner une conséquence négative. Dans les faits, une source authentique disposera en effet d'un "monopole". Afin de limiter autant que possible les risques que cela implique, la Commission plaide pour que :

    a. pour chaque source authentique, un "comité d'utilisateurs" soit créé, afin que ces utilisateurs aient également une participation dans le fonctionnement et la politique de la source authentique. Un tel système veillera d'ailleurs également à ce que :

        i. la source authentique puisse évoluer selon les besoins qui se présenteront au cours de son développement ultérieur ;

        ii. les obligations, procédures et processus mis au point par la source authentique soient mieux exécutés et de façon plus efficace (cf. infra les points 28-29) ;

    b. les données issues des sources authentiques soient en principe mises gratuitement à la disposition d'autres instances publiques, ce pour que l'utilisation des données ne soit pas freinée et que le principe de la source authentique ne soit pas annihilé.

3) Exactitude des données

17. La Commission estime que l'exactitude des données contenues dans une source authentique est un élément crucial. Si la source authentique contient des données fautives, ces dernières seront rapidement diffusées partout et "contamineront" toutes sortes de traitements de données dans le secteur public. Ce phénomène est également appelé "diffusion de la pollution"[11]. Un tel scénario doit absolument être évité.

18. À cet effet, la Commission formule les recommandations suivantes :

[11] G. Overkleeft-Verburg, "Basisregistraties en rechtsbescherming. Over de dualisering van de bestuurlijke rechtsbetrekking", Nederlands Tijdschrift voor Bestuursrecht 2009, p. 80.

a. des procédures claires doivent être définies et mises en œuvre tout au long des quatre phases.
   Dans ce cadre, des Service Level Agreements (SLA) peuvent aussi être conclus (par ex. des accords entre la source authentique et une (des) instance(s) chargée(s) de la collecte des données) ;

b. la phase de validation doit être assurée par une instance qui :
   i. dispose des moyens nécessaires à cet effet ;
   ii. a elle-même intérêt à ce qu'une validation minutieuse ait lieu.
   Lorsque cette double condition est remplie, on peut raisonnablement s'attendre à une validation de qualité ;

c. pour autant que ce soit nécessaire en vue des finalités avancées, l'historique des données doit être tenu à jour. De cette manière, une consultation d'informations qui étaient authentiques à un moment donné dans le passé est toujours possible ;

d. dans la source authentique, il faut travailler avec des identifiants sur la base desquels les personnes concernées peuvent être identifiées sans qu'aucune confusion avec d'autres personnes concernées ne soit possible (ex. : des identifiants uniques tels que le numéro d'identification du Registre national[12]) ;

e. des procédures doivent être élaborées pour la correction des erreurs :

   i. une procédure par laquelle les utilisateurs (instances) et/ou les personnes concernées (les citoyens) doivent signaler des erreurs[13].
   À titre d'exemple, la Commission renvoie en la matière au modèle néerlandais, dans le cadre duquel une "obligation de notification" s'applique[14]. Cela implique qu'un utilisateur qui a un 'doute fondé'[15] sur

---

[12] Pour autant qu'une autorisation ait été obtenue à cet effet.

[13] L'article 4, alinéa 3 de la loi du 8 août 1983 *organisant un Registre national des personnes physiques* prévoit d'ailleurs déjà une forme (limitée) de notification en ce qui concerne le Registre national : *"(…) Quiconque constate une différence entre les informations du Registre national et les informations contenues dans les registres visés à l'article 2* [= les registres de population]*, doit le communiquer sans délai."*

[14] https://wiki.stelselvanbasisregistraties.nl/xwiki/bin/view/Stelselhandboek/terugmelden.

[15] *"On parle d'un doute fondé sur l'exactitude d'une donnée si les critères suivants sont remplis :*

1. Une (forte) présomption qu'une donnée (authentique) est inexacte.

2. Un doute fondé sur l'exactitude d'une donnée authentique peut exclusivement provenir d'une observation effectuée par l'organe public dont émane la notification, observation selon laquelle la réalité ne correspond pas à l'enregistrement.

3. La présomption doit reposer sur quelque chose (présomption fondée). La notification doit être motivée (par exemple en invoquant une enquête ou un contrôle dans le cadre de l'exécution des tâches).

4. On parle de doute fondé si le client arrive à la conclusion qu'une notification conduira plus que probablement à une modification de la donnée authentique.

l'exactitude des données qu'il a réclamées auprès d'une source authentique est obligé de notifier ce doute à la source authentique. La source authentique est toujours obligée soit d'examiner elle-même la notification et de corriger d'éventuelles erreurs, soit de transmettre le cas échéant cette notification à l'instance chargée de la collecte/validation des données[16] afin que celle-ci puisse assurer le suivi ultérieur ;

ii. une procédure permettant à la source authentique de rectifier des erreurs dans la source de sa propre initiative ou à la demande d'instances chargées de la collecte/validation des données ;

iii. une procédure permettant à la source authentique de notifier aux utilisateurs des erreurs qui ont été détectées[17] ;

f. il importe de bien définir le contenu des données reprises dans une source authentique, afin que les utilisateurs puissent établir avec certitude, sur la base de la définition, si une donnée authentique peut bel et bien être utilisée dans le contexte qu'ils envisagent.

En outre, dans certains cas, il peut être recommandé de répartir les données en plusieurs sous-catégories plutôt que de les enregistrer comme une seule donnée. La "notion de rémunération" dans le secteur de la sécurité sociale en est ici une bonne illustration : il est plus efficace de conserver les différentes parties du dossier de la rémunération séparément étant donné que certains éléments de ce dossier font partie de la "rémunération", alors que cela n'est pas le cas dans un autre contexte ;

g. des "cross-controls" peuvent éventuellement être organisés (croisement avec d'autres banques de données afin de détecter des erreurs).

19. Enfin, à cet égard, on peut faire remarquer que le principe de collecte unique de données et de partage des données a de plus en plus souvent pour effet que pour (certaines) des données authentiques, une (sorte d') "obligation d'utilisation" est d'application. Le décret flamand du 18 juillet 2008 *relatif à l'échange électronique de données administratives*

---

5. Il s'agit de faits qui sont contradictoires et incompatibles" [traduction libre réalisée par le Secrétariat de la Commission, en l'absence d'une traduction officielle]

(https://wiki.stelselvanbasisregistraties.nl/xwiki/bin/view/Stelselhandboek/Gerede+twijfel)

Voir également : www.bprbzk.nl/dsresource?objectid=36239&type=org.

[16] Ce pour les cas où l'erreur signalée concerne des traitements qui relèvent de la responsabilité de l'instance chargée de la collecte ou de la validation des données et pas de la responsabilité de la source authentique elle-même.

[17] Cette notification s'inscrit d'ailleurs dans la logique de l'article 12, § 3 de la LVP (en matière de droit de rectification) qui stipule que "*(…) le responsable du traitement communique les rectifications ou effacements des données (…) aux personnes à qui les données incorrectes (…) ont été communiquées (…)*".

semble aller dans cette direction (article 3, alinéa 1 dudit décret)[18]. L'article 6 de la loi du 8 août 1983 *organisant un Registre national des personnes physiques* prévoit également une "obligation d'utilisation"[19].

20. Une des raisons d'instaurer une obligation d'utilisation est la garantie d'une bonne qualité de données. Le raisonnement suivi est en effet que la fréquence de l'utilisation des données aura une sorte d' "effet autonettoyant" sur la banque de données. Toutefois, tout le monde n'est pas convaincu que cela suffira pour assurer une bonne qualité des données.

21. La Commission estime qu'une telle obligation d'utilisation, combinée à "l'obligation de notification" susmentionnée, peut contribuer à une plus grande exactitude des données. Cependant, cette mesure ne suffira pas toujours à garantir l'exactitude des données dans la source authentique. La Commission plaide dès lors pour que plusieurs mesures (comme par exemple les mesures énumérées au point 18) soient toujours mises en œuvre simultanément.

22. La Commission insiste également sur le fait que l'instauration d'une "obligation d'utilisation" ne peut pas avoir pour conséquence de passer outre au principe de finalité (cf. supra les points 9 et suivants).

4) Transparence

23. Les traitements de données qui ont lieu lors des quatre phases doivent avant tout être transparents à l'égard des personnes concernées (les citoyens). En la matière, la Commission considère qu'il y a trois points importants :

    a. remplir l'obligation d'information au sens de l'article 9 de la LVP ;

    b. prévoir des procédures accessibles[20] à tous via lesquelles les personnes concernées peuvent aisément exercer leurs droits (droit d'accès/de rectification, …). La Commission fait remarquer à cet égard qu'une personne concernée doit

[18] Le décret flamand prévoit toutefois un certain nombre d'exceptions (article 2, 2° et article 3, alinéa 2 dudit décret).

[19] "*§ 1er. Les autorités, les organismes et les personnes (…) qui sont autorisés à consulter les données du Registre national, ne peuvent plus demander directement lesdites données à une personne.*

§ 2. Dès qu'une donnée a été communiquée au Registre national et enregistrée dans ledit Registre, la personne concernée n'est pas tenue de la communiquer directement aux autorités, organismes et personnes (…) qui sont autorisés à consulter les données du Registre national."

[20] Les procédures doivent également préciser l'instance à laquelle la personne concernée doit s'adresser. Dans de nombreux cas, il s'agira de la source authentique, mais il peut également s'agir par exemple de l'instance chargée de la collecte et/ou de la validation des données (si la collecte ne se fait pas par la source authentique).

toujours[21] pouvoir vérifier qui a eu accès à quel moment à quelles données les concernant ;

c. Lorsqu'une décision est prise à l'égard d'un citoyen, l'instance prenant la décision doit toujours indiquer à la personne concernée sur quelles données elle s'est basée, où celles-ci ont été réclamées et auprès de qui le citoyen peut exercer ses droits (voir le point b). De cette manière, le citoyen a encore la possibilité, le cas échéant, de prouver que certaines données ne sont pas (plus) correctes.
Dans ce cadre, la Commission rappelle également l'article 12*bis* de la LVP, sur la base duquel *une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut* en principe *être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité*[22].

24. La Commission recommande également de prévoir à l'égard des utilisateurs des données authentiques une certaine transparence. Ainsi, la source authentique pourrait rendre publique la description exacte des (catégories de) données qu'elle gère. En outre, il importe aussi d'établir des structures claires (par ex. systématiser les données qui sont proposées par la source authentique) et des procédures stables à travers le temps à l'égard d'un utilisateur.

5) Sécurité

25. La Commission souligne l'importance d'une politique de sécurité adéquate pour chaque source authentique. À cet égard, elle renvoie tout d'abord à ses *Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel*[23]. De plus, elle attire l'attention sur sa recommandation n° 01/2008 du 24 septembre 2008 *relative à la gestion des accès et des utilisateurs dans le secteur public* et sur le principe des 'cercles de confiance' exposé aux points 13-15 de la recommandation n° 03/2009 du 1er juillet 2009 *concernant les intégrateurs dans le secteur public*.

26. La Commission estime également que chaque source authentique doit disposer d'un conseiller en sécurité de l'information.

---

[21] Ce qui n'implique pas que le responsable du traitement doive réagir immédiatement à une telle demande. Il suffit que cela se fasse dans un délai raisonnable.

Par ailleurs, le but ne peut pas non plus être qu'une personne concernée puisse exiger cette vérification au sujet de consultations ayant eu lieu longtemps auparavant. Il serait en effet contraire à l'article 4, § 1, 5° que ce type de données soient conservées pour une durée indéterminée.

[22] La personne concernée doit pouvoir communiquer son point de vue avant qu'une décision définitive ne soit prise.

[23] http://www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf.

6) Autorisations

27. La Commission souligne que les règles en matière d'autorisations doivent être respectées dès que certains flux de données sont opérationnalisés. La loi a en effet créé au sein de la Commission des comités sectoriels qui sont compétents pour examiner au préalable des traitements de données déterminés et se prononcer dans les limites fixées par la loi[24].

7) Remarque finale

28. La Commission insiste sur le fait qu'une source authentique doit définir des responsabilités claires à tous niveaux (exactitude des données, sécurité, transparence, délais de conservation, etc.). À cet effet, il faut élaborer les procédures et les SLA nécessaires et intégrer des mécanismes de contrôle afin de vérifier si les procédures mises en place sont respectées.

29. La source authentique doit donc remplir pour les quatre phases un rôle actif et de coordination, et ce également pour les (aspects des) phases pour lesquelles elle n'est pas elle-même directement ou complètement responsable.

L'Administrateur f.f., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere

[24] À titre d'exemple :

- l'article 42, § 2, 3° de la loi du 13 décembre 2006 *portant dispositions diverses en matière de santé* (tel que modifié par l'article 70, 3° de la loi du 1er mars 2007 *portant des dispositions diverses (III)*), entré en vigueur par arrêté royal du 7 octobre 2009 *fixant la date et les modalités d'entrée en vigueur de l'article 70, 3°, de la loi du 1er mars 2007 portant des dispositions diverses (III)* ;

- l'article 36*bis* de la LVP ;

- l'article 11 du décret du 18 juillet 2008 *relatif à l'échange électronique de données administratives*.