Les sources authentiques de données

Burnet, Christine

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2014

Document Version
le PDF de l'éditeur

Les sources authentiques de données – L'Accord de coopération du 23 mai 2013

Christine Burnet[1]

Le développement des technologies de l'information et de la communication permet aux autorités publiques d'envisager un mode de fonctionnement différent, favorisant notamment le partage de données entre administrations. L'application du principe de collecte unique rend ce partage de données incontournable. En effet, dès lors qu'une même donnée est nécessaire à plusieurs autorités publiques, cette donnée doit être collectée par l'une d'entre elles et mise ensuite à la disposition des autres. La base de données reprenant cette donnée est une source authentique de données, un concept dont le déploiement nécessite la mise en place d'un cadre garantissant l'équilibre entre efficacité des services publics et protection de la vie privée des usagers. En Belgique, différents textes règlent cette matière dont 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. L'analyse de cet Accord fait l'objet de la présente contribution.

• • •

The ICT development creates new opportunities for public administrations which imply a new way of working based, among others, on data sharing. Due to the application of the 'unique data collection principle', this sharing is becoming inevitable. As soon as a data is processed by several public authorities, it has indeed to be collected by one of them which then shares it with the other authorities. The database that contains this data is called 'authentic data source'. The development of such sources requires a specific frame to ensure that efficiency of public authorities and privacy of the citizens are well-balanced. In Belgium, this matter is regulated by several legal instruments among which the «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». The present paper presents and analyses the content of this Agreement.

INTRODUCTION

Le concept de source authentique de données est apparu en Belgique avec la mise à disposition des autorités publiques de nouveaux moyens techniques issus des technologies de l'information et de la communication (TIC).

Le développement des échanges par voie électronique a favorisé le passage d'une administration initialement structurée «en silos», dans laquelle les différents services gèrent des bases de données cloisonnées, à une administration

[1] L'auteure remercie Cécile de Terwangne, Elise Degrave, Karen Rosier, Axel Lefebvre et Laurent Noël pour leur relecture approfondie et le partage de leurs connaissances sur le sujet.

qui organise un accès à l'information coordonné entre les différents services. On parle dès lors d'e-gouvernement intégré.

Concrètement, les administrations fédérales, régionales, communautaires, provinciales et communales collectent des données auprès des usagers, personnes physiques et morales, dans le cadre de l'exercice de leurs missions. Certaines données ainsi collectées sont transversales car utilisées par différentes autorités ou par différents services d'une même autorité, il semble donc évident d'optimiser leur traitement en mutualisant les ressources par la mise en place de processus communs ; c'est ici qu'intervient la source authentique de données.

La source authentique se présente comme un ensemble de données collectées par une instance qui met ces données à la disposition d'autres instances préalablement autorisées à les consulter par un organe spécifique.

Le but de la présente contribution est de présenter le concept de source authentique tel qu'organisé par l'Accord de coopération du 23 mai 2013 et de mettre en évidence l'importance de la qualité des données échangées par le biais des sources authentiques.

Après avoir présenté l'Accord de coopération du 23 mai 2013 dans un premier chapitre, nous aborderons la définition de la notion de source authentique dans le second chapitre. Nous envisagerons dans le troisième chapitre les opportunités et risques que leur utilisation engendre et nous nous attarderons finalement sur la qualité des données échangées par le biais des sources authentiques dans un quatrième chapitre.

I. PRÉSENTATION DE L'ACCORD DE COOPÉRATION DU 23 MAI 2013

La Région wallonne et la Communauté française ont signé le 23 mai 2013 un Accord de coopération portant sur le développement d'une initiative commune en matière de partage de données et sur la gestion conjointe de cette initiative[2] [3].

Cet Accord se fonde sur l'article 77 de la loi spéciale du 8 août 1980 de réformes institutionnelles qui permet au Gouvernement de la Communauté française et au Gouvernement de la Région wallonne de régler leur coopération mutuelle et d'organiser des services communs et il se fonde également sur l'article 92*bis* de la même loi spéciale qui permet aux Communautés et Régions de conclure des accords de coopération qui portent notamment sur la création et la gestion conjointes de services et institutions communes, sur l'exercice de compétences propres, ou sur le développement d'initiatives en commun.

Comme il porte sur des matières réglées par décret, l'Accord de coopération du 23 mai 2013 n'a eu d'effet qu'après avoir reçu l'assentiment de la Communauté française par décret du 4 juillet 2013[4] et de la Région wallonne par décret du 10 juillet 2013[5].

2 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, *M.B.*, 23 juillet 2013, p. 46031.

3 Ci-après dénommé « Accord de coopération du 23 mai 2013 ».

4 Décrets du 4 juillet 2013 portant assentiment à 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, *M.B.*, 23 juillet 2013, p. 46007.

5 Décrets du 10 juillet 2013 portant assentiment à 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

Ce texte « s'applique à tout échange de données issu de sources authentiques de données, de banques de données issues de sources authentiques ou de sources authentiques externes dans la limite des compétences de la Région wallonne et de la Communauté française »[6].

Il a vocation à régler les échanges de données entre autorités wallonnes et francophones ainsi qu'entre ces autorités et une autorité appartenant au niveau international ou fédéral, entre ces autorités et une autorité d'une autre Région ou Communauté ou d'une institution ou personne morale qui en relèvent et entre ces autorités et une personne morale de droit privé qui est chargée de tâches ou de missions d'intérêt général.

Il apparaît important que les différentes législations et réglementations applicables à ces échanges assurent une coordination efficace entre les autorités et visent par conséquent une interopérabilité maximale[7]. Conscientes de cette nécessité, les administrations fédérales, régionales et communautaires ont conclu un Accord de coopération[8] dont l'objectif est d'harmoniser et aligner les initiatives des différentes parties afin de réaliser un e-gouvernement intégré. Ce dernier rappelle les principes et composants d'un e-gouvernement intégré et organise la coopération entre les parties, en citant notamment les sources authentiques, sans en donner de définition, tel n'est d'ailleurs pas son objet.

Toutefois, l'utilisation de définitions sinon identiques, *a minima* compatibles, semble être la base indispensable à la mise en place d'un accès intégré aux sources authentiques.

Nous allons donc débuter par ce préliminaire important dans le prochain chapitre et analyser la définition de source authentique telle que prévue dans l'Accord de coopération pour la comparer avec les définitions issues d'autres réglementations belges.

II. DÉFINITION DE LA NOTION DE SOURCE AUTHENTIQUE

La notion de source authentique a fait l'objet de définitions antérieures à l'Accord de coopération. Même si elles présentent des différences, ces définitions recouvrent approximativement un concept unique.

Le point 2 de l'article 2 du décret flamand du 18 juillet 2008 définit la source authentique comme « un fichier de données, tenu de manière électronique, qui a été identifié par le Gouvernement flamand comme étant le plus complet et de qualité supérieure, et qui est utile ou nécessaire dans le cadre de l'échange électronique de données administratives »[9].

Cette première définition parle de fichier de données, il met l'accent sur la nature des données qu'il contient et sur la reconnaissance de la source authentique par le Gouvernement flamand.

Ensuite, aux termes des points 5 et 6 de l'article 2 de la loi du 15 août 2012, une source authentique est une « banque de données dans laquelle sont conservées des données

de partage de données et sur la gestion conjointe de cette initiative, *M.B.*, 23 juillet 2013, p. 46027.

6 Accord de coopération du 23 mai 2013, précité au n° 2, article 3.

7 À ce sujet, voy. H. Kubicek et R. Cimander, « Three dimensions of organisational interoperability – Insights from recent studies for improving interoperability frameworks », *European Journal of ePractice*, 2009, pp. 3-14.

8 Accord de coopération du 26 août 2013 entre les administrations fédérales, régionales et communautaires afin d'harmoniser et aligner les initiatives visant à réaliser un e-gouvernement intégré, *M.B.*, 8 octobre 2013, p. 70727, article 1er.

9 Décret flamand du 18 juillet 2008 relatif à l'échange électronique de données administratives, *M.B.*, 29 octobre 2008, p. 57325, article 2, 2°.

authentiques »[10] à savoir une « donnée récoltée et gérée par une instance dans une base de données et qui fait foi comme donnée unique et originale concernant la personne ou le fait de droit concerné, de sorte que d'autres instances ne doivent plus collecter cette même donnée »[11].

Dans cette définition apparaît en filigrane le principe de collecte unique[12] dont la source authentique est un corollaire. Ce principe prévoit qu'une donnée ne doit être recueillie qu'une seule fois auprès de l'usager à condition que les exigences de protection des données et de la vie privée soient satisfaites. La donnée authentique, unique et originale, est collectée par une seule instance. Les autorités publiques organisent en conséquence un système d'information structuré afin d'échanger entre elles les données récoltées par l'une d'elles auprès de l'usager.

Nous verrons plus tard que le fait de devoir respecter les exigences de protection de la vie privée contraint certaines autorités à ne pas appliquer ce principe et à collecter elles-mêmes des données déjà collectées par une autre autorité. La protection de la vie privée met donc à mal le principe de collecte unique.

Finalement, la définition prévue au point 1 de l'article 2 de l'Accord de coopération du 23 mai 2013 mentionne qu'une source authentique est une « base de données instituée en vertu d'un décret ou d'un arrêté de Gouvernement d'une des parties contenant les données relatives à des personnes physiques ou morales, qui ont 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 »[13].

Il convient de décomposer cette troisième définition afin de dégager les éléments essentiels de la notion de source authentique.

A. La procédure de désignation d'une source authentique

La définition de l'Accord de coopération, à l'instar de celle du décret du 18 juillet 2008, inclut dans les caractéristiques de la source authentique, le fait qu'elle ait été préalablement instituée par un décret ou un arrêté de gouvernement. Seules les bases de données existantes peuvent faire l'objet de la procédure de désignation et devenir sources authentiques. L'Accord de coopération ne mentionne pas de critère supplémentaire.

Il nous semble que la procédure de désignation d'une source authentique devrait automatiquement comprendre la vérification de critères prédéfinis, transparents et, autant que possible, mesurables.

Pour exemple, le Gouvernement flamand a posé comme critère le fait d'offrir des « garanties suffisantes quant à

– la qualité des données, en particulier l'exhaustivité, l'exactitude, l'actualité, les garanties en matière d'assurance de la qualité des données, en matière de contrôle de la

10 Loi du 15 août 2012 relative à la création et à l'organisation d'intégrateur de services fédéral, *M.B.*, 29 août 2012, p. 53170, article 2, 6°.

11 Loi du 15 août 2012, précitée au n° 10, article 2, 5°.

12 Accord de coopération du 28 septembre 2006 entre l'État fédéral, les Communauté flamande, française et germanophone, la Région flamande, la Région wallonne, le 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 octobre 2006, p. 55747, article 2, 2.

13 Accord de coopération du 23 mai 2013, précité au n° 2, article 2, 1°.

qualité à l'égard des clients, la traçabilité des modifications de données et la sauvegarde de l'historique de l'accès aux données ;
– l'utilité de la source authentique, notamment l'accessibilité et la publicité ;
– le caractère opérationnel de la source de données, notamment la disponibilité ;
– la sécurité de la source de données au niveau physique, technique et organisationnel »[14].

Cette méthode permet de limiter les risques de contestation liés à la décision de désignation. En effet, la décision de transformer une base de données en source authentique entraîne des conséquences non négligeables, notamment en termes de moyens pour l'autorité qui en assume la gestion. Il est donc préférable que cette décision soit motivée par des éléments objectifs.

Par ailleurs, en terme d'interopérabilité, soulignons qu'aucune procédure de reconnaissance de sources authentiques existantes n'a été prévue, or les flux de données ne seront pas limités aux sources authentiques désignées en vertu de l'Accord de coopération du 23 mai 2013.

B. L'objet des données authentiques

La donnée est au centre de la notion de source authentique, dont l'appellation complète est source authentique de données. Les données contenues dans les sources authentiques peuvent avoir divers objets dont notamment des personnes physiques ou morales, des biens meubles ou immeubles, mais aussi des faits. Parmi ces données, certaines sont des données à caractère personnel dont le traitement est régi par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (LVP)[15], d'autres ne le sont pas.

L'Accord de coopération du 23 mai 2013 précise que les données contenues dans une source authentique sont relatives aux personnes physiques ou morales. Il est intéressant de comparer cet élément de la définition avec son équivalent dans les deux autres définitions proposées, tandis que la loi précise des « données (…) concernant la personne ou le fait de droit concerné »[16], le décret flamand fait simplement référence à des « données »[17].

Quelles sont finalement les données concernées ?

Toutes les données réclamées auprès des usagers par l'administration pour accomplir ses missions sont visées par le principe de collecte unique. Celui-ci s'applique indépendamment de l'objet de la donnée, et les sources authentiques, étant une application de ce principe, ne peuvent donc voir leur champ d'application limité à certaines données. Toutes les données collectées par les autorités peuvent être contenues dans une source authentique.

Quant au fait qu'une donnée soit à caractère personnel, il a un impact majeur puisqu'il détermine si la LVP est applicable ou non mais le lien entre source authentique et LVP ne revêt pas de caractère automatique.

La Commission de la protection de la vie privée (C.P.V.P.) estime dans sa recommandation 09/2012 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

14 Arrêté du Gouvernement flamand du 15 mai 2009 portant exécution du décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, *M.B.*, 14 juillet 2009, p. 48881, article 2, §1er.

15 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801.

16 Loi du 15 août 2012 précitée, article 2, 5°.

17 Décret du 18 juillet 2008, précité, article 2, 2°.

source authentique, il convient donc de veiller à ce que la LVP soit rigoureusement respectée » et ajoute que « l'application de la LVP à un concept relativement nouveau et abstrait tel que celui des sources authentiques ne va toutefois pas de soi »[18]. Une source authentique peut contenir des données qui ne sont pas des données à caractère personnel.

De la même manière que le principe de collecte unique n'est pas limité en fonction de l'objet des données, il ne l'est pas plus en fonction du caractère personnel ou non des données.

C. La collecte des données authentiques

Comme nous l'avons déjà souligné[19], les sources authentiques sont une conséquence du principe de collecte unique qui vise à limiter les collectes de données par les autorités publiques auprès des usagers.

L'article 8 de l'Accord de coopération du 23 mai 2013 prévoit qu'après avoir été autorisées à consulter les données contenues dans une source authentique, les autorités publiques ne peuvent plus organiser de collecte directe de ces données[20]. La collecte directe doit laisser la place à la collecte indirecte, par l'intermédiaire des sources authentiques.

Nous déduisons de la *ratio legis* de cet article que la collecte directe constitue l'exception, y compris pour les autorités publiques qui n'ont pas été autorisées à consulter les données de la source authentique. En effet, si seules les autorités autorisées à consulter les données contenues dans une source authentique se voient imposer la collecte indirecte, d'autres peuvent éviter cette obligation en n'introduisant pas de demande d'autorisation d'accès.

Toutes les autorités publiques utilisant une donnée contenue dans une source authentique doivent donc introduire une demande d'autorisation d'accès à cette source authentique.

Lorsque la collecte indirecte est impossible pour des raisons juridiques ou techniques, l'autorité publique peut effectuer une collecte directe si les dispositions de la LVP sont respectées.

Citons l'exemple d'une demande d'accès à une source authentique refusée au motif que la finalité est incompatible avec la finalité de la collecte initiale effectuée par la source authentique mais dont la finalité est conforme aux dispositions de la LVP. La collecte indirecte est impossible mais la collecte directe peut être envisagée.

La collecte de la même donnée sera donc effectuée auprès des usagers par plusieurs autorités publiques. Il est important que l'autorité de contrôle veille à ne pas laisser perdurer ce type de situation, au risque de mettre en péril le concept de source authentique.

Une collecte directe ne respectant pas les dispositions de la LVP ne peut par contre pas être effectuée. Citons l'exemple d'une collecte dont la finalité est illégitime.

L'article 3 du décret du 18 juillet 2008 prévoit que « Les entités de l'administration flamande doivent recueillir les données dont elles ont besoin pour développer l'échange électronique de données administratives, auprès de sources authentiques de données. Uniquement si, pour des raisons techniques ou juridiques, il est impossible de recueillir une donnée auprès d'une source authentique de données, ou s'il n'existe pas de source authentique de données, les entités de l'administration flamande recueillent des données auprès de l'utilisateur »[21].

18 C.P.V.P., recommandation n° F-20120523-6 (9/2012) du 23 mai 2012, p. 2/11.

19 Voy. p. 30.

20 On parle de collecte directe lorsqu'elle est effectuée auprès des usagers.

21 Décret du 18 juillet 2008 relatif à l'échange électronique de données administratives, *M.B.*, 29 octobre

La rédaction de cet article va dans le sens de l'interprétation qui est donnée ci-dessus à l'article 8 de l'Accord de coopération du 23 mai 2013.

D. Le gestionnaire de source authentique

L'autorité publique qui est responsable de la source authentique est désignée ou reconnue par la réglementation. Ce sera le cas des sources authentiques désignées conformément à l'article 7, paragraphe 1er de l'Accord de coopération du 23 mai 2013. Elle peut également être « implicitement soutenue par la réglementation »[22]. C'est le cas du registre national qu'aucun texte ne qualifie de source authentique mais qui en présente toutes les caractéristiques.

Une autorité publique qui assume la responsabilité de la source authentique dans le cadre de l'Accord de coopération est appelée gestionnaire de source authentique.

Notons que seules les autorités publiques, définies au point 8 de l'article 2 de l'Accord de coopération du 23 mai 2013, peuvent assurer les différentes phases du traitement des sources authentiques. Cette solution limite les acteurs susceptibles de participer au développement des sources authentiques mais présente des garanties en termes de pérennité.

La réalisation des opérations (collecte, stockage, mise à jour et destruction des données) peut être répartie entre plusieurs acteurs, c'est le cas des communes qui sont chargées de la collecte et de la validation des données relatives au registre national des personnes physiques.

Outre le respect des obligations découlant de la LVP, dont notamment l'obligation d'assurer la qualité des données ainsi que leur sécurité[23] ou l'obligation de donner suite à une notification d'erreur, le gestionnaire de source authentique doit mettre en place des moyens techniques permettant aux personnes concernées d'exercer leurs droits d'accès et de rectification par voie électronique[24].

On le voit, la fonction de gestionnaire de source authentique nécessite la mise à disposition de moyens qui doivent être adéquatement évalués avant que ne soit prise la décision de désignation.

E. La réutilisation des données authentiques

À terme, les données ne seront plus collectées qu'une seule fois auprès des usagers, il semble donc évident qu'elles seront réutilisées par les autorités n'ayant pas effectué de collecte mais ayant à traiter ces données pour assurer leur mission. Nous analyserons plus tard le risque lié à l'incompatibilité des traitements ultérieurs.

Plus les données contenues dans une source authentique sont réutilisées, plus cette source authentique a de raison d'être[25]. L'outil de travail d'une autorité publique devient un outil de travail collectif. Cela implique que son gestionnaire garde à l'esprit ce caractère collectif lors du développement de fonctionnalités. Il sera en effet tenu par les garanties à offrir en matière d'accessibilité, notamment.

On peut également penser que plus une donnée est réutilisée plus grande est sa qualité, car les occasions de constater une éventuelle inexactitude et de la corriger sont

2008, p. 57325, article 3, alinéa 1er et alinéa 2.

22 C.P.V.P., recommandation n° F-20120523-6 (9/2012) du 23 mai 2012, p. 3/11.

23 Accord de coopération du 23 mai 2013, précité au n° 2, article 10, § 1er.

24 Accord de coopération du 23 mai 2013, précité au n° 2, article 9, § 1er.

25 Il ne semble en effet pas justifié de désigner comme source authentique une base de données dont les données servent au seul gestionnaire de cette source authentique.

plus nombreuses, mais nous verrons dans un prochain chapitre que cet effet autonettoyant[26] ne suffit pas à garantir l'exactitude des données échangées.

III. OPPORTUNITÉS ET RISQUES DES SOURCES AUTHENTIQUES

Nous citons ci-après les opportunités liées au développement des sources authentiques. Les risques engendrés et les mesures prévues par l'Accord de coopération du 23 mai 2013 pour les limiter feront ensuite l'objet de commentaires.

A. Opportunités

Les sources authentiques présentent des avantages, tant pour les usagers que pour les services publics. L'approche « win-win » est d'ailleurs envisagée dans l'Accord de coopération du 26 août 2013[27] visant la réalisation d'un e-gouvernement intégré qui, tant du point de vue de l'usager que du point de vue de l'administration, contribue à accroître la qualité et l'efficacité des services publics tout en bénéficiant d'économies d'échelle.

D'une part les usagers sont moins sollicités par les autorités publiques. Les données les concernant étant partagées, elles sont accessibles sous certaines conditions à toutes les autorités publiques sans que les usagers aient à les répéter à différents interlocuteurs. Leurs démarches s'en trouvent allégées, et idéalement simplifiées.

D'autre part, les autorités publiques gagnent en efficacité. En effet, elles ne doivent plus multiplier les demandes aux usagers pour obtenir une même donnée. Une fois la donnée collectée, elle est, moyennant le respect de conditions, accessible auprès de la source authentique. Le temps de traitement des dossiers par les autorités publiques s'en trouve donc réduit. Ce nouvel outil nécessite une adaptation des méthodes de travail, considérée comme une « opportunité car elle fournit aux administrations une occasion de repenser leurs modes opératoires en assurant leurs missions en phase avec les besoins réels des usagers »[28].

Par ailleurs, les redondances d'information sont réduites et la qualité de l'information s'en trouve améliorée, elle gagne en cohérence et homogénéité.

B. Risques

L'application du principe de collecte unique et la création de sources authentiques présentent également des risques, structurels et fonctionnels.

1. Incompatibilité des traitements ultérieurs

La question de la compatibilité des traitements ultérieurs est inhérente à la notion de source authentique puisque les données contenues dans une source authentique ont vocation à être réutilisées. Or il est évident que les finalités poursuivies lors de cette réutilisation ne seront pas identiques aux finalités initiales qui ont motivé la collecte de ces données, les premières devront néanmoins être compatibles avec les secondes[29].

La C.P.V.P. envisage dans sa recommandation 09/2012 le fait « qu'une zone de tension puisse apparaître entre, d'une part la collecte unique et, d'autre part, l'article 4, § 1er, 2°, de la LVP aux termes duquel des données collec-

26 C.P.V.P., recommandation n° F-20120523-6 (9/2012) du 23 mai 2012, p. 9/11.

27 Accord de coopération du 26 août 2013, précité au n° 8.

28 Accord de coopération du 23 mai 2013, précité au n° 2.

29 E. Degrave, « Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée », *Chroniques de droit public*, 2009, pp. 46-71.

tées pour des finalités déterminées, explicites 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 avoir pour effet de passer outre l'article 4, § 1er, 2°, de la LVP ».

Basé sur cette recommandation, l'article 4, paragraphe 1er de l'Accord de coopération du 23 mai 2013 précise que « la transformation d'une base de données existante en une source authentique implique que les données qu'elle contient seront diffusées à d'autres autorités publiques et réutilisées par celles-ci, à d'autres fins que celles qui étaient poursuivies par la collecte initiale. Ces diffusions et réutilisations de données sont des traitements ultérieurs, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel ».

Il appartient à la Commission Wallonie-Bruxelles de Contrôle des échanges de données (C.C.E.D.) de vérifier cette compatibilité et d'une manière générale de s'assurer que les dispositions de la LVP soient respectées[30].

La C.C.E.D., créée par les articles 22 et suivants de l'Accord de coopération, a pour mission de veiller au respect des dispositions de l'Accord de coopération du 23 mai 2013 relatives à l'échange des données de sources authentiques de manière homogène dans la Région wallonne et la Communauté française. Sa composition, incluant trois membres de l'ordre linguistique francophone de la C.P.V.P., assure une certaine cohérence entre les avis, recommandations et autorisations des deux instances. Toutefois, bien que l'Accord de coopération du 23 mai 2013 soit entré en vigueur au 1er janvier 2014, la création de la C.C.E.D. n'a pas été concomitante.

2. *Sécurité de l'information*

L'utilisation des sources authentiques a pour conséquence d'augmenter les échanges de données, de sorte que les risques d'atteinte à la sécurité des données s'en trouvent multipliés.

Pour assurer la sécurité des données échangées, il est important de réfléchir en amont de la désignation à l'architecture des sources authentiques afin d'équilibrer la répartition de la collecte des données entre les différentes autorités publiques et de mettre en place une politique de sécurité adéquate.

En aval de la désignation, l'Accord de coopération du 23 mai 2013 impose au gestionnaire de source authentique d'assurer la sécurité des données (article 10, paragraphe 1er) et à tout utilisateur, c'est-à-dire à toute autorité publique qui a accès aux sources authentiques, de désigner un conseiller en matière de sécurité de l'information (article 12, paragraphe 3).

Par ailleurs, la sécurité des données sera un des aspects envisagés par la C.C.E.D. pour toute demande d'autorisation d'accès à des données à caractère personnel d'une source authentique qui lui sera soumise conformément à l'article 23 de l'Accord de coopération du 23 mai 2013.

3. *Situation monopolistique*

L'application du principe de collecte unique engendre des risques liés à la création d'un monopole dans le chef de l'administration responsable de la source authentique.

Dans la mesure où la source authentique est, en principe, incontournable, son accessibilité doit être assurée pour éviter que les autorités publiques ne puissent exercer leur mission parce que les données nécessaires à cet exercice ne sont pas accessibles. La C.P.V.P. a d'ail-

30 Y. Poullet et E. Degrave, « La création d'une institution en charge de la protection des données au sein de la Communauté française et/ou de la Région wallonne », *R.D.T.I.*, n° 33, 2008, pp. 427-429.

leurs souligné à ce propos que les utilisateurs doivent recevoir « des garanties que le mode d'accessibilité des données a été établi de façon stable de manière à ce que leurs activités ne soient pas inutilement perturbées et à ce que des adaptations et donc des investissements ne soient pas sans cesse nécessaires pour maintenir l'accès ouvert »[31].

Ensuite, la situation monopolistique peut générer des tensions entre les autorités publiques, voire des réactions négatives de la part des autorités publiques n'ayant pas obtenu la reconnaissance de leur base de données comme source authentique. En effet, dès lors que l'on considère l'information comme une ressource, le fait d'être contraint de la partager entraîne des difficultés culturelles qu'il faut surmonter. Afin d'éviter ce type de contestation, il importe de définir des critères de sélection d'une source authentique et que ces critères soient basés sur des mesures quantifiables.

Enfin, l'Accord de coopération du 23 mai 2013 prévoit en son article 7 que « les données sont accessibles aux autorités publiques gratuitement »[32]. Il suit en cela la recommandation de la C.P.V.P. qui, afin de limiter les effets négatifs liés à la création d'un monopole, souligne l'importance de la gratuité de l'accès aux données même si elle reconnaît que, « la gratuité de principe a toutefois ses limites et il ne faut pas exclure que cela aura, dans certains cas, un effet contre-productif, par exemple parce que le responsable du traitement tentera d'éviter une reconnaissance de certaines de ses données comme authentiques »[33].

L'article 7 de l'Accord de coopération du 23 mai 2013 ne précise pas si la désignation d'une source authentique nécessite l'accord de l'autorité publique dont la base de données est transformée en source authentique. Certaines autorités publiques peuvent en effet ne pas souhaiter cette désignation.

4. Complexité des sources authentiques et de leur architecture

Le concept de source authentique et l'architecture qui se met en place autour de ce concept peuvent paraître de prime abord rebutants. Pour les autorités publiques habituées à traiter des données qu'elles collectent elles-mêmes, elles doivent dorénavant identifier exactement la donnée nécessaire et la source authentique qui la contient, en demander l'accès, autant d'étapes qui peuvent en rendre certaines réticentes et les inciter à faire jouer les exceptions pour éviter d'y recourir. Ensuite, ce concept peut poser des difficultés aux gestionnaires de source authentique qui ont des obligations à remplir et dont la charge de travail augmente significativement.

Il a donc semblé opportun de créer une plateforme d'échange de données commune à la Région wallonne et à la Communauté française. Cette plateforme ayant une mission d'assistance générale aux sources authentiques se nomme la Banque-Carrefour d'échanges de données (B.C.E.D.).

La B.C.E.D. est instituée en vertu des articles 11 et suivants de l'Accord de coopération du 23 mai 2013. Elle est définie comme une « structure instituée par le présent accord de coopération pour être

a) un tiers de confiance, c'est-à-dire une entité indépendante de confiance qui offre des services qui accroissent la fiabilité de l'échange électronique de données et de l'enregistrement de données et qui n'a elle-

31 C.P.V.P., avis n° F-20130626-2 du 26 juin 2013, n° 23/2013, p. 9/13.

32 Accord de coopération du 23 mai 2013, précité au n° 2, article 7.

33 C.P.V.P., avis n° F-20130626-2 du 26 juin 2013, n° 23/2013, p. 10/13.

même aucune mission ou aucun intérêt en matière de traitement réel de fonds de données à caractère personnel ;

b) un intégrateur de services, c'est-à-dire une institution légalement reconnue dont le rôle principal et d'organiser et de faciliter l'échange de données issues de sources authentiques ou de banques 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 »[34].

La C.P.V.P. préconise également que la B.C.E.D. joue un rôle d'intégrateur de données, consistant à agréger des données provenant de plusieurs sources authentiques et à les enregistrer dans une banque de données intégrées distincte, en vue de les communiquer à des tiers[35].

Attribuer ce rôle à la B.C.E.D. semble discutable. En vertu de l'article 13 de l'Accord de coopération du 23 mai 2013, la B.C.E.D. est autorisée à effectuer, sous conditions, une copie cache des données qu'elle reçoit de sources authentiques externes. L'article 15 du même Accord prévoit que la B.C.E.D. peut « fournir aux autorités publiques des services supplémentaires comme l'agrégation de données provenant de différentes sources authentiques » et « héberger des données issues de sources authentiques pour le compte des sources authentiques qui ne disposeraient pas des capacités matérielles ou techniques pour héberger et exposer leurs données ». Or ces deux articles visent une agrégation et un enregistrement temporaires effectués pour rendre plus efficace la transmission ultérieure de l'information et non pour créer une nouvelle banque de données. Nous ne pouvons donc en déduire que le rôle d'intégrateur de services de la B.C.E.D. se prolonge par celui d'intégrateur de données.

Comme le résume la C.P.V.P., la B.C.E.D. « a pour but de simplifier et d'optimiser les échanges de données entre les différents acteurs publics en mettant particulièrement l'accent sur l'utilisation des données authentiques »[36].

Pour lui permettre d'atteindre cet objectif, l'Accord de coopération du 23 mai 2013 prévoit que « la Banque-Carrefour d'échanges de données (B.C.E.D.) gère conformément à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, un répertoire de références indiquant les instances auprès desquelles des types déterminés de données sont conservés concernant des personnes, entreprises ou institutions déterminés ou qui fait référence à la source de données où ces données peuvent être consultées ou qui, par personne physique ou entreprise, indique quels types de données sont mis à disposition d'instances ou d'autorités externes déterminées et pour quelle période, avec mention du but pour lequel l'instance ou l'autorité externe a besoin de ces données et gérer un répertoire d'autorisations qui stipule qui a accès, sous quelles conditions, à des données déterminées »[37].

La B.C.E.D. a indéniablement un rôle à jouer pour garantir la transparence des traitements de données.

Pour renforcer le rôle de la B.C.E.D., l'article 6 de l'Accord de coopération du 23 mai 2013 rend obligatoire la consultation de données accessibles par son intermédiaire. En effet, les autorités publiques autorisées à accéder à

34 Accord de coopération du 23 mai 2013, précité au n° 2, article 2, 3°.

35 C.P.V.P., recommandation n° F-20090701-3 (03/2009) du 1er juillet 2009, p. 2/16.

36 C.P.V.P., avis n° F-20120912-11 (29/2012) du 12 septembre 2012, p. 15/29.

37 Accord de coopération du 23 mai 2013, précité au n° 2, article 11, § 2, h).

une source authentique accessible par le biais de la B.C.E.D. ne peuvent plus collecter les données concernées par l'autorisation auprès des usagers mais doivent les consulter auprès de la B.C.E.D.

C. Les sources authentiques, sources de qualité

La collecte étant, en principe[38], unique, aucun contrôle ne pourra s'opérer par une autre autorité collectant la même donnée. Si des cas de collectes multiples sont toujours possibles, ils doivent demeurer exceptionnels. La donnée, unique, fruit de l'application du principe de collecte unique, se doit donc d'être exacte afin de limiter les risques de contamination vers l'ensemble des services utilisant la même donnée.

Alors qu'une donnée erronée était presque uniquement utilisée par les services qui la collectaient, une donnée authentique erronée a vocation à circuler davantage puisqu'elle peut être communiquée à tout service justifiant des conditions imposées par l'organisme de contrôle compétent.

Pour qualifier l'effet domino ainsi généré, la C.P.V.P. parle du phénomène de « diffusion de la pollution »[39].

La croissance exponentielle de la quantité de données échangées et le caractère obligatoire du recours aux sources authentiques rendent la problématique de qualité des données de plus en plus importante, particulièrement lorsqu'elles concernent des données à caractère personnel.

Après avoir précisé comment l'exactitude des données est envisagée dans la LVP, nous analyserons différentes mesures pouvant être adoptées pour améliorer la qualité des données contenues dans les sources authentiques.

1. Le principe d'exactitude posé par la loi vie privée

La LVP prévoit que « les données à caractère personnel doivent être : […] exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées »[40].

Le responsable du traitement doit mettre en œuvre toutes les mesures raisonnables pour effacer ou rectifier des données inexactes ou incomplètes, il doit donc mettre en œuvre toutes les mesures raisonnables pour éviter ces erreurs ou les détecter. En effet, l'exactitude des données ne peut être assurée que par la mise en place de mesures préventives, de mesure d'identification des erreurs et de mesures de correction de ces erreurs.

L'article 10 de l'Accord de coopération du 23 mai 2013 précise les obligations qui incombent aux gestionnaires de sources authentiques, dont l'obligation d'assurer la qualité des données.

2. La qualité des données comme critère de désignation

Comme nous l'avons déjà évoqué, le législateur flamand a inscrit la qualité des données comme critère de désignation d'une source authentique.

La C.P.V.P. suggère de considérer la qualité des données comme un critère permettant de désigner le gestionnaire de source authentique : « lorsqu'il faut faire un choix entre différents responsables du traitement qui collectent la

38 Voy. p. 32.

39 C.P.V.P., recommandation n° F-20120523-6 (9/2012) du 23 mai 2012, p. 6/11.

40 Loi du 8 décembre 1992, précitée au n° 15, article 4, § 1er, 4°.

même donnée, il va de soi qu'il faut préférer le responsable qui offre le plus de garanties en matière d'exactitude »[41].

Cela suppose que la qualité des données puisse être évaluée de manière objective, sur la base d'indicateurs de mesure définis. Cette analyse doit certes se faire en amont de la désignation auprès des autorités publiques « candidates » mais elle doit également être réalisée en aval afin de vérifier si le niveau de qualité des données demeure satisfaisant.

Une labellisation des sources authentiques est envisageable, sur base de critères précis et effectuée par une instance présentant des garanties d'indépendance[42].

3. *La qualité des données via une démarche « Quality of Data »*

La C.P.V.P., consciente de l'importance de la qualité des données, a formulé des recommandations[43] intégrées en partie dans les différents textes légaux et réglementaires relatifs à cette matière. Par ailleurs, des analogies peuvent être faites entre le concept de source authentique et celui d'ERP[44], c'est-à-dire un système unifié permettant à des utilisateurs de différents métiers de travailler dans un environnement qui repose sur une base de données unique. Les solutions mises en place dans le secteur privé par les entreprises utilisant des ERP peuvent également inspirer le secteur public.

La mise en place de nouveaux outils de gestion de l'information s'accompagne idéalement d'une adaptation des méthodes de travail. On parle de démarche QoD (« Quality of Data ») dont l'aboutissement se trouve dans l'établissement d'une gouvernance des données. Le maître mot de cette gouvernance est la responsabilisation des gestionnaires de sources authentiques et de leurs utilisateurs.

Les points à aborder au cours de cette démarche sont :

a) l'analyse des processus liés à la collecte, la validation, la gestion et la mise à disposition des données incluant
   - la rédaction de procédures relatives aux quatre phases ;
   - l'utilisation d'identifiants permettant d'éviter toute confusion entre les usagers ;
   - la conclusion de « Service level agreement »[45] entre la source authentique et l'instance chargée d'une phase du traitement ;
   - la validation des données par une instance qui dispose de moyens nécessaires à cet effet et qui a elle-même un intérêt à ce qu'une validation minutieuse ait lieu ;

b) la description des données selon une systématique déterminée[46].
   La définition des éléments constitutifs des données contenues dans la source authentique est primordiale. En effet, un libellé identique peut recouvrir des informations différentes en fonction du contexte. La description des données permet donc aux autorités publiques d'identifier avec exactitude la donnée nécessaire et de contrôler dans quelle mesure la donnée ou plusieurs éléments constitutifs sont pertinents pour leurs activités ;

41 C.P.V.P., avis n° F-20130626-2 (23/2013) du 26 juin 2013, p. 7/13.

42 C.P.V.P., avis n° F-20120912-11 (29/2012) du 12 septembre 2012, p. 12/29.

43 C.P.V.P., recommandation n° F-20120523-6 (9/2012) du 23 mai 2012, p. 7/11 ; avis n° F-20130626-2 (23/2013) du 26 juin 2013, p. 8/13.

44 Abréviation de « Enterprise Resource Planning », c'est-à-dire un progiciel de gestion intégrée.

45 Aussi appelé « SLA », c'est-à-dire un accord dans lequel le service et le niveau de qualité attendu sont définis par les parties.

46 C.P.V.P., avis n° F-20130626-2 (23/2013) du 26 juin 2013, p. 9/13.

c) la détection d'erreurs par la mise en place d'audits et de « cross-controls » (croisements avec d'autres banques de données) ;
d) l'obligation de notification : l'article 10, paragraphe 2, de l'Accord de coopération du 23 mai 2013 oblige le destinataire des données qui constate que les données sont imprécises, incomplètes ou inexactes, de le communiquer immédiatement au gestionnaire de sources authentiques, lequel a l'obligation d'y donner suite. Le fait de considérer la source authentique comme un outil de travail collectif rend évidente cette obligation de notification. Elle institutionnalise la collaboration entre le gestionnaire de la source authentique et ses utilisateurs ;
e) la correction d'erreurs avec notamment
   – 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 ;
   – une procédure permettant à la source authentique de notifier aux destinataires de données des erreurs qui ont été détectées.

On le voit, les mesures à mettre en place pour assurer l'exactitude des données sont nombreuses et à combiner, compte tenu des spécificités de chaque source authentique, aucune ne pouvant garantir à elle seule un niveau de qualité maximal.

4. La qualité des données grâce à la participation des usagers

L'usager est apte à juger de l'exactitude des données le concernant. Le faire participer au processus de validation des données constitue donc une mesure complémentaire pour assurer la qualité des données échangées.

Cette implication des usagers peut se faire soit dans le cadre de la publicité passive des autorités publiques, c'est-à-dire lorsque l'usager en prend l'initiative en exerçant un droit d'accès, soit dans le cadre de la publicité active, c'est-à-dire lorsque les autorités publiques prennent l'initiative de la communication d'informations aux usagers.

5. Exercice des droits d'accès et de rectification

Dans le cadre de la LVP, l'usager peut demander la correction de l'erreur constatée sur base de l'article 12, paragraphe 1er qui prévoit que « toute personne a le droit d'obtenir sans frais la rectification de toute donnée à caractère personnel inexacte qui le concerne »[47].

Toutefois, pour juger de l'exactitude d'une donnée, il faut que l'usager en ait connaissance. Le droit de rectification aurait peu d'intérêt, s'il ne s'accompagnait pas du droit d'accès.

La LVP prévoit un droit d'accès en son article 10 : « La personne concernée qui apporte la preuve de son identité a le droit d'obtenir du responsable du traitement b) la communication sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données »[48].

Dans le cadre des sources authentiques, l'exercice de ce droit par les usagers peut s'avérer compliqué car il nécessite l'identification préalable de l'instance concernée, ou encore de par la multiplicité des instances à contacter. La C.P.V.P. constate qu'« il faut à tout prix éviter que le citoyen soit découragé d'exercer ses droits parce qu'il lui est impossible d'identifier le(s) bon(s) interlocuteur(s) »[49].

Consciente de cette difficulté, elle recommande de « prévoir des procédures accessibles

47 Loi du 8 décembre 1992, précitée au n° 15, article 12, §1er.
48 Loi du 8 décembre 1992, précitée au n° 15, article 10.
49 C.P.V.P., recommandation n° F-20090701-3 (03/2009) du 1er juillet 2009, p. 6/16.

à tous via lesquelles les personnes concernées peuvent aisément exercer leurs droits »[50].

L'Accord de coopération du 23 mai 2013 suit cette recommandation et prévoit, pour les personnes concernées, « la possibilité d'accéder par voie électronique aux données à caractère personnel les concernant et détenues par la B.C.E.D., lorsque celles-ci sont disponibles sous forme électronique, et aux informations concernant les traitements automatiques de ces données »[51].

6. *Vers une obligation positive de communication des données aux usagers*

L'exercice du droit d'accès et du droit de rectification nécessite une démarche des usagers, on parle de publicité passive (dans le chef des administrations).

À l'opposé, une forme de publicité active consisterait en la communication par les administrations de l'ensemble des données contenues dans les sources authentiques au sujet d'un usager, afin qu'il puisse être informé des données qui le concernent et exercer son droit de rectification si cela s'avère nécessaire.

Entre la publicité active et la publicité passive, le choix des autorités publiques semblait clair. À l'image de l'évolution de l'article 20 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, détaillée par E. Degrave[52].

Cet article prévoyait initialement une obligation de communiquer d'office certaines données au bénéficiaire concerné et il a été remplacé par une obligation de motivation formelle. Or comme l'a indiqué la C.P.V.P., « l'obligation de motivation formelle n'a pas tout à fait le même but que l'obligation de communiquer d'office certaines données à caractère personnel »[53]. En effet, dans certains cas, les données disponibles seront plus nombreuses que celles qui doivent être communiquées pour respecter l'obligation de motivation formelle car toutes les données disponibles concernant un usager ne sont pas nécessaires pour prendre une décision à son sujet.

Si l'on considère que l'information des usagers a notamment pour objectif d'améliorer la qualité des données, il est pourtant nécessaire de leur communiquer un maximum de données tout en veillant au respect de mesures de sécurité particulières afin de ne transmettre à chaque usager que les données qui le concernent et qui peuvent lui être communiquées.

L'Accord de coopération du 23 mai 2013 vise à assurer une information aussi complète que possible des usagers. La C.P.V.P. constate avec satisfaction que le principe de transparence des traitements de données est prévu par l'intermédiaire des articles 8, paragraphe 2 et paragraphe 3 de cet Accord[54].

D'une part, l'article 8, paragraphe 2, stipule que l'autorité publique qui effectue une collecte de données, précise aux usagers les données qu'elle consulte à leur propos auprès de sources authentiques. De cette manière, les usagers ont connaissance de l'ensemble des données qui seront traitées par cette autorité publique.

D'autre part, l'article 8, paragraphe 3, prévoit que les autorités publiques « pré-remplissent les demandes d'informations adressées à des personnes, entreprises, organismes ou institutions au moyen de données obtenues auprès

50 C.P.V.P., recommandation n° F-20120523-6 (9/2012) du 23 mai 2012, p. 9/11.

51 Accord de coopération du 23 mai 2013, précité au n° 2, article 17.

52 E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, coll. Crids, Bruxelles, Larcier, 2014, n° 318.

53 C.P.V.P., avis n° F-19960205-1 (05/96) du 5 février 1996, p. 3.

54 C.P.V.P., avis n° F-20120912-11 (29/2012) du 12 septembre 2012, p. 13/29.

de sources authentiques ou de banques de données issues de sources authentiques. Elles indiquent dans ce cas l'origine des données ». De cette manière, l'usager réduit certes le temps nécessaire au traitement du formulaire mais il peut surtout vérifier l'exactitude des données pré-remplies le concernant.

Idéalement, vu le développement des outils techniques dont disposent les autorités publiques, nous imaginons une déclaration de données dressée conjointement par les autorités publiques et adressée périodiquement par voie électronique à tout usager. Il s'agirait d'une simple communication aux usagers destinée à leur permettre d'en vérifier le contenu. Le droit de rectification étant laissé à l'initiative des usagers ayant constaté une anomalie.

Les moyens techniques qui sont à la disposition des autorités publiques et des usagers pour assurer la qualité des données se complètent et l'évolution des TIC permettra certainement d'en développer davantage.

CONCLUSION

Le développement des TIC a permis l'émergence de nouveaux outils de travail, utiles pour tous, y compris pour les autorités publiques. Voici une formidable opportunité de gagner en efficacité, d'alléger les formalités et de simplifier les démarches des usagers.

Le partage de l'information n'a en soi rien d'innovant mais il a profité de l'évolution technologique pour s'imposer, générer le concept de source authentique qui permet d'organiser une gestion partagée de l'information entre les autorités publiques.

Ce concept se développe au sein de toutes les autorités publiques, avec des spécificités juridiques qui ne doivent pas constituer un frein à son développement. Pour gagner en homogénéité et garantir un niveau de sécurité de l'information et de protection de la vie privée équivalent, il donc est primordial que le développement des sources authentiques fasse l'objet d'échanges et de coordination entre toutes les autorités publiques concernées.

Il est clair que les apports indéniables de ce concept peuvent être anéantis si les risques qu'il contient ne sont pas anticipés, notamment en matière de qualité des données. Conscient des différents dangers qu'implique le partage de l'information, le législateur a pris les mesures nécessaires pour garantir la protection de la vie privée et la sécurité de l'information. Certaines mesures favorisant la transparence pourraient les compléter avantageusement. En effet, les usagers ont encore un accès limité à l'information qui les concerne, ils peuvent certes exercer les droits qui leur sont reconnus mais, soyons objectifs, seuls les initiés le font. Pourtant, la participation des usagers aux processus de gestion des données administratives présente de nombreux avantages, que ce soit au niveau de la perception qu'ils ont des autorités publiques ou de l'acceptation des décisions de ces dernières.

Dans le contexte actuel, la gestion des données ne peut plus être appréhendée sans tenir compte de l'importance de la confiance des personnes concernées. Pour garantir cette confiance, il est nécessaire d'impliquer raisonnablement ces dernières dans le processus de gestion des données.