Recommandation n°02/2010 du 31 mars 2010

Objet : recommandation concernant le rôle de protection de la vie privée des Trusted Third Parties (TTP ou tiers de confiance) lors de l'échange de données (A/2009/022)

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 l'arrêté royal du 13 février 2001 *portant exécution 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* (ci-après "l'arrêté royal du 13 février 2001") ;

Vu le rapport du Président ;

Émet, le 31 mars 2010, la recommandation suivante :

I. INTRODUCTION

1. Le "Trusted Third Party" (ci-après "TTP"), également appelé "Third Trusted Party", "tiers de confiance" ou "médiateur de confiance" est "*an entity trusted by multiple other entities within a specific context and which is alien to their internal relationship*"[1] [2].

2. La notion de "TTP" est utilisée dans des contextes souvent très différents. La Commission a également déjà émis plusieurs avis dans lesquels il était question d'un "TTP". Généralement, il s'agissait de remarques indirectes dans le cadre de dossiers spécifiques. La présente recommandation vise une approche plus systématique et plus intégrale du TTP. Ainsi, la Commission souhaite en particulier examiner dans quels cas l'intervention d'un tel TTP peut offrir une plus-value au niveau de la protection de la vie privée.

II. LE "TRUSTED THIRD PARTY" EN DROIT BELGE

3. Le "TTP" est une notion qui couvre de nombreux aspects[3]. Le législateur belge a choisi de réglementer un certain nombre de TTP spécifiques. La loi du 15 mai 2007 *fixant un cadre juridique pour certains prestataires de services de confiance* prévoit notamment des règles pour les fonctions de TTP suivantes[4] :

- service d'archivage électronique ;
- service d'horodatage électronique ;
- service de recommandé électronique ;
- service de blocage transitoire des sommes versées.

4. La Commission reconnaît que ces TTP peuvent offrir une plus-value pour certains aspects ponctuels de protection de la vie privée. Le "service d'horodatage électronique" pourra par exemple contribuer à l'exactitude des données (cf. article 4, § 1, 4° de la LVP) et le "service de recommandé électronique" pourrait être considéré, dans certains traitements de données, comme un élément de l'application de l'article 16 de la LVP (sécurité).

---

[1] Page 16 du Consultation paper du 23/11/2005 on "*Common Terminological Framework for Interoperable Electronic Identity Management*" (https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc#4_44_Trusted_third_party_TTP).

[2] Il ne s'agit que d'une des définitions possibles du concept de "TTP".

[3] À titre d'exemple, on peut faire référence à une étude néerlandaise, qui peut être consultée via le lien suivant : http://www.cbpweb.nl/downloads_av/AV22.pdf?refer=true&theme=purple.

[4] Cf. J. Dumortier et G. Somers, "De wet van 15 mei 2007 tot vaststelling van een juridisch kader voor sommige verleners van vertrouwensdiensten: een eerste verkenning", *T.B.H.* 2007/7, p. 649-659.

5. Néanmoins, ces fonctions de TTP ne seront pas approfondies ci-après. Dans la présente recommandation, la Commission souhaite en effet se concentrer sur les cas où un TTP intervient en tant que maillon lors de l'échange de données à caractère personnel et où cette intervention s'inspire de manière structurelle de considérations de protection de la vie privée.

III. TRUSTED THIRD PARTIES EN TANT QUE PROTECTEURS DE LA VIE PRIVÉE LORS D'UN ÉCHANGE DE DONNÉES

6. La Commission voit six cas où les motifs de recourir à un "TTP" lors d'un échange de données s'inscrivent tout à fait dans le cadre de la protection de la vie privée. Ces cas sont expliqués ci-après de manière méthodique.

A. Un TTP qui anonymise des données

7. Un TTP peut se charger d'anonymiser des données à caractère personnel. Étant donné la définition de "données anonymes" [5], cela implique que lorsque le TTP a rempli sa mission d'anonymisation, les données qu'il a traitées ne peuvent plus, en aucune façon, être mises en relation avec une personne physique, même pas par lui.

B. Un TTP qui code les données

8. Un TTP peut également coder des données. Un codage de données à caractère personnel doit être vu comme une transformation des données afin qu'elles ne puissent plus être mises en relation avec une ou plusieurs personnes identifiées ou identifiables sans que le destinataire final des données connaisse les techniques de transformation utilisées.

9. Le terme "code" désigne donc les mécanismes de transformation et les paramètres éventuels utilisés dans la transformation. À titre d'exemple, on peut faire référence aux techniques suivantes :

- "hasardisation" d'une donnée : remplacement d'une donnée par une donnée aléatoire ou arbitraire (par exemple : remplacer un numéro d'identification par un numéro séquentiel d'introduction du dossier ou par un nombre généré aléatoirement) ;
- permutation de données : échange de deux données de deux individus différents au sein d'une même catégorie (par exemple : échange des dates de naissance de deux personnes

[5] *"données anonymes" : les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont donc pas des données à caractère personnel* (article 1, 5° de l'arrêté royal du 13 février 2001).

nées dans la même dizaine d'années). La permutation peut également être opérée entre plus de deux individus ;

- algorithme de calcul : remplacement d'une donnée par une autre calculée sur la première (par exemple : hachage ou remplacement du numéro d'identification par un code de Hash réversible ou non) ;
- brouillage de données : remplacement des données par d'autres à l'aide d'un algorithme logique ou mathématique et ces données sont obtenues par des opérations faites sur une ou plusieurs données de plusieurs cas de l'échantillon.

C. Un TTP qui agrège des données

10. Lors de l'agrégation de données, ces dernières sont rassemblées en groupes, rendant (presque) impossible l'identification des personnes individuelles sur la base des résultats fournis par le TTP.

11. À titre d'exemple : supposons qu'un chercheur veuille savoir combien de nouveaux cas de cancer du poumon ont été constatés en 2008 et dans quelle catégorie d'âge ce diagnostic a été le plus souvent posé. Dans ce cas, le chercheur n'a pas besoin de données à caractère personnel détaillées. Il lui suffit de recevoir un chiffre du nombre total de cas par âge. Une intervention d'un TTP peut fournir ce résultat. Des données agrégées donnent donc des renseignements sur les résultats à des niveaux 'supérieurs' aux diagnostics individuels.

D. Un TTP qui se charge du contrôle des accès ou y participe

12. La Commission a déjà affirmé à plusieurs reprises – notamment dans l'avis n° 30/98 du 25 septembre 1998 – que les membres des professions pour lesquelles il existe un ordre ou une instance à compétence disciplinaire ne pourraient accéder au Registre national que via l'intermédiaire de cette instance. Les personnes qui souhaitent un accès pourraient communiquer à cette dernière le motif de la consultation – permettant un contrôle de la finalité de la consultation – et l'instance en question pourrait également vérifier si cette personne n'a subi aucune peine disciplinaire (un élément que le gestionnaire d'une source authentique ne peut généralement pas examiner). Le TTP agit donc comme un premier filtre contre un usage abusif.

13. Une telle approche peut considérablement améliorer la gestion des utilisateurs et des accès de sources authentiques[6]. L'ordre (ou une autre instance à compétence disciplinaire) – qui agit en

[6] Voir également à cet égard la recommandation n° 01/2008 du 24 septembre 2008.

tant que TTP – fonctionne en tant que gardien de l'utilisation légitime par ses membres d'une source authentique comme le Registre national. Il est garant du fait que celui qui consulte une source authentique est également réellement en fonction et il veille aussi, en outre, à la finalité des consultations. De cette façon, le secteur lui-même peut organiser un contrôle de sa propre organisation.

14. La Commission attire également l'attention, dans ce contexte, sur les tâches des intégrateurs telles que visées dans la recommandation n° 03/2009 du 1er juillet 2009, étant donné qu'ils peuvent également jouer un rôle important dans l'organisation de la gestion des utilisateurs et des accès de sources authentiques, mais d'une autre manière que les ordres (ou les autres instances à compétence disciplinaire)[7].

E. Un TTP qui aide à l'envoi de documents sans publier l'identité des personnes concernées

15. À titre d'exemple, on peut faire référence au rôle du Registre national dans le cadre de la prise de contact en vue de réunions, de commémorations ou de la recherche d'un membre de la famille dont il est question dans la recommandation n° 02/2009 du 27 mai 2009. Dans ladite recommandation, il est suggéré aux services du Registre national – sous certaines conditions – d'apporter leur concours à la localisation de personnes pour des raisons sociales ou humanitaires, plus précisément en transmettant les lettres d'un demandeur sans lui communiquer l'adresse du destinataire. Le demandeur atteint ainsi son but, à savoir faire parvenir son message au destinataire, et dans un même temps, la vie privée du destinataire est respectée. Ce dernier décide en effet lui-même s'il reprend contact avec le demandeur et, le cas échéant, s'il communique son adresse actuelle.

---

[7] À titre d'exemple, on peut faire référence à la délibération n° 36/2006 du 20 décembre 2006 et à la délibération n° 08/031 du 3 juin 2008, dans lesquelles CORVE a été autorisée, respectivement par la Commission de la protection de la vie privée, en lieu et place du Comité sectoriel du Registre national, et par le Comité sectoriel de la Sécurité sociale et de la Santé, Section "Sécurité sociale", à accéder à des données à caractère personnel du Registre national des personnes physiques et des registres de la Banque-carrefour de la sécurité sociale pour pouvoir accomplir sa tâche en tant que volet de transmission des données à caractère personnel concernées au profit des applications cibles flamandes. Chaque recherche effectuée par une application cible flamande est loggée par CORVE. C'est CORVE qui contrôle l'accès aux données à caractère personnel et qui veillera à ce que les données à caractère personnel provenant du Registre national des personnes physiques et des registres de la Banque-carrefour soient exclusivement communiquées ultérieurement aux services compétents respectifs de l'autorité flamande, conformément aux autorisations en vigueur, définies par ou en vertu de la loi ou par une décision du comité sectoriel compétent de la Commission de la protection de la vie privée. Tant la Commission elle-même que le Comité sectoriel de la Sécurité sociale et de la Santé sont favorables à une telle méthode étant donné qu'elle augmente la garantie d'une exécution correcte des décisions d'autorisation.

16. Un autre exemple concerne le rôle intermédiaire du Registre national lors de la transmission d'enquêtes écrites à des personnes d'un échantillon[8]. S'il s'agit de questionnaires écrits[9] destinés à une enquête unique, le Registre national le chargera lui-même de l'envoi des questionnaires et d'une lettre d'introduction, certes sur la base du matériel fourni par l'organisme de recherche. Les envois ultérieurs peuvent se faire en utilisant la même procédure. Dans ce cas, le Registre national ne transmet à l'organisme de recherche que les informations – sous forme codée – nécessaires pour permettre l'analyse des refus de répondre.

IV. CONDITIONS AUXQUELLES DOIVENT SATISFAIRE LES TTP

A. Conditions auxquelles tous les TTP qui sont mentionnés sous le titre III de la présente recommandation doivent satisfaire

17. La Commission recommande que tous les TTP qui font l'objet de la présente recommandation respectent les principes suivants :

- le TTP – avec le ou les autres responsable(s) du traitement (ultérieur) – doit veiller de manière générale au respect correct de la législation en matière de protection de la vie privée.
  Cela implique également que lorsqu'un TTP constate que les traitements de données dans lesquels il intervient menacent de ne pas se dérouler, sur certains points, conformément à la LVP, il est recommandé qu'il le signale au(x) responsable(s) du traitement (ultérieur), même s'il s'agit d'aspects du traitement pour lesquels il n'est pas lui-même (tout à fait) responsable d'un point de vue juridique. À cet égard, la Commission pense en particulier au respect des principes de finalité et de proportionnalité et au respect de l'obligation de déclaration et/ou de l'obligation ou des obligations d'autorisation ;

- le TTP ne peut pas utiliser les données qu'il a traitées dans le cadre de sa (ses) fonction(s) de TTP pour d'autres finalités que les finalités spécifiques qui lui ont été confiées ;

- un TTP doit prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la

[8] Cf. avis d'initiative n° 27/2008 du 3 septembre 2008 et l'addendum identique au vade-mecum "Vie privée : le vade-mecum du chercheur" que la Commission a publié en octobre 2008 (première édition).

[9] "*Les enquêtes écrites sont la règle, les enquêtes orales l'exception. Si le chercheur n'est pas en mesure ou ne souhaite pas travailler avec un questionnaire écrit, il doit en demander l'autorisation en introduisant une demande motivée auprès du Comité sectoriel* (du Registre national)."

perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. Concrètement, cela implique notamment :

- qu'un TTP ne peut octroyer un accès aux données qui font l'objet d'un couplage qu'à des personnes spécialement désignées par lui et qu'il doit soumettre ces personnes à une obligation de confidentialité. Elles ne peuvent consulter les données que si cela est nécessaire pour que le TTP puisse remplir sa mission.
  Un TTP doit également dresser une liste de ces personnes qu'il doit pouvoir présenter sur demande éventuelle de la Commission, surtout si les données soumises au traitement sont celles dont il est question aux articles 6 à 8 inclus de la LVP (cf. article 25 de l'arrêté royal du 13 février 2001) ;

- que le TTP doit de préférence désigner, au sein ou non de son personnel, un conseiller en sécurité de l'information et en protection de la vie privée ;

- qu'un TTP doit s'organiser selon les cercles de confiance[10] ;

➢ les traitements effectués par un TTP doivent se dérouler de manière transparente. Cela implique notamment que :

- les responsables du traitement initial et/ou du traitement ultérieur doivent au moins recevoir du TTP les informations suivantes :
  - le fonctionnement du TTP et les conditions d'utilisation des services du TTP ;
  - la portée de la responsabilité du TTP.
- les personnes concernées doivent toujours – sur la base des informations fournies par le TTP et par les responsables du traitement initial et/ou du traitement ultérieur – pouvoir savoir auprès de qui elles peuvent exercer leur droit d'accès, de rectification, de suppression ou de non utilisation.

B. <u>Conditions supplémentaires pour les TTP qui anonymisent des données (cf. titre III, point A de la présente recommandation)</u>

18. Outre les conditions générales exposées ci-dessus (cf. le point 17 susmentionné), un TTP qui anonymise des données doit également spécifiquement tenir compte des directives suivantes :

[10] Cf. recommandation n° 03/2009, points 13-15.

- un TTP doit détruire les données à caractère personnel qui lui ont été transmises par les responsables du traitement initial dès qu'il a accompli sa mission d'anonymisation, à moins qu'il ne s'agisse d'une mission dont il découle qu'il doit conserver les données ;

- un TTP doit utiliser tous les moyens techniques pour rendre impossible une identification éventuelle des personnes concernées par le responsable du traitement (ultérieur).

C. Conditions supplémentaires pour les TTP qui codent des données (cf. titre III, point B de la présente recommandation)

i. Un TTP qui code des données et qui intervient en tant qu' "organisation intermédiaire" au sens du Chapitre II de l'arrêté royal du 13 février 2001

19. Le TTP est souvent utilisé comme synonyme de l'expression "organisation intermédiaire" (ci-après "OI") au sens de l'article 1, 6° de l'arrêté royal du 13 février 2001[11]. Ce même Chapitre II de l'arrêté royal reprend un certain nombre de garanties[12]. Il s'agit plus précisément des règles suivantes :

- une OI doit être suffisamment indépendante vis-à-vis du responsable du traitement ultérieur (le destinataire des données codées)[13].
  Selon la Commission, cette indépendante peut être obtenue de plusieurs manières. Cela est évidemment possible en faisant exercer la fonction d'OI par une instance qui n'a aucun lien avec le traitement de données dans lequel le TTP intervient.
  Une autre possibilité est le cas où l'OI est gérée ou dirigée par un groupe d'utilisateurs. Le fait qu'un de ces utilisateurs puisse avoir un intérêt dans des cas concrets n'hypothèque pas nécessairement l'indépendance de l'OI, étant donné que le poids commun des autres utilisateurs peut garantir l'indépendance dans de telles situations ;

---

[11] À titre d'exemple, voir : K. Van Gossum et G. Verhenneman, "De informatisering van de kankerregistratie in België", *Computerrecht* 2008, p. 281.

[12] La Commission précise que l'expression "organisation intermédiaire" dans le Chapitre II de cet arrêté royal du 13 février 2001 doit être interprétée de manière plus limitée que la notion de "TTP". Le rôle d'une OI se limite au codage de données à caractère personnel dans le cadre de traitements ultérieurs à des fins historiques, statistiques ou scientifiques (ci-après "fins HSS") qui, en soi, ne sont pas compatibles avec les finalités de la collecte initiale de données. Dans ce contexte, l'OI se charge uniquement de convertir des données à caractère personnel non codées en données codées, au profit d'un responsable du traitement ultérieur à des "fins HSS". Par contre, un "TTP" peut par exemple intervenir en dehors du contexte d'un traitement ultérieur (voir également ci-dessous aux points 30 et suivants).

[13] Article 11 de l'arrêté royal du 13 février 2001.

- une OI doit prendre les mesures techniques et organisationnelles appropriées pour empêcher la conversion de données codées en données non codées[14] ;

- une OI ne peut communiquer des données codées, en vue de leur traitement ultérieur à des fins historiques, statistiques ou scientifiques, que sur présentation, par le responsable du traitement ultérieur, de l'accusé de réception d'une déclaration complète faite auprès de la Commission[15] ;

- le responsable du traitement initial de données à caractère personnel ou l'OI doit, préalablement au codage de données sensibles, judiciaires ou relatives à la santé (articles 6-8 de la LVP), communiquer aux personnes concernées certaines informations[16], sauf si :
  - cette obligation se révèle impossible ou implique des efforts disproportionnés[17] ou
  - l'OI est une autorité administrative chargée explicitement, par ou en vertu de la loi, de rassembler et de coder des données à caractère personnel et soumise, à cet égard, à des mesures spécifiques visant à protéger la vie privée, instituées par ou en vertu de la loi[18].

  Le responsable du traitement initial ou l'OI qui souhaite coder de telles données sans notification préalable à la personne concernée complète la déclaration auprès de la Commission avec des informations déterminées ; après quoi, la Commission émet une recommandation[19].

20. La Commission recommande également que les TTP qui codent des données et interviennent en tant qu'OI – outre les directives générales décrites ci-dessus par la Commission (cf. le point 17 susmentionné) – utilisent tous les moyens techniques pour rendre impossible une identification éventuelle des personnes concernées par le responsable du traitement (ultérieur). Concrètement, cela implique notamment :

- qu'il faut prévoir une protection particulière des méthodes et/ou des paramètres utilisés lors du codage ;

---

[14] Article 12 de l'arrêté royal du 13 février 2001.

[15] Article 13 de l'arrêté royal du 13 février 2001.

[16] Article 14 de l'arrêté royal du 13 février 2001.

[17] Article 15, premier alinéa de l'arrêté royal du 13 février 2001.

[18] Article 15, deuxième alinéa de l'arrêté royal du 13 février 2001.

[19] Article 16 de l'arrêté royal du 13 février 2001.

- que le TTP doit toujours veiller à ce que les données codées mises à disposition ne soient pas trop détaillées au point qu'une réidentification soit possible. Une telle réidentification peut en effet être possible en reliant les données fournies par le TTP entre elles ou en les associant à des informations dont le destinataire dispose déjà.

21. La Commission profite aussi de l'occasion pour confirmer ou, au contraire, infirmer un certain nombre de thèses qui sont parfois adoptées concernant l'intervention d'une OI. Il s'agit plus précisément des thèses suivantes :

a. une OI doit également toujours être indépendante du (des) *fournisseur(s)* de données ;
b. l'intervention d'une OI n'est nécessaire que lorsque des données des différents fournisseurs de données concernent les mêmes personnes physiques.

22. La thèse adoptée au point a. va trop loin. En effet, l'article 11 de l'arrêté royal du 13 février 2001 n'impose une obligation d'indépendance pour les OI qu'à l'égard du responsable du traitement ultérieur (le destinataire des données codées). Si une OI agit en tant que sous-traitant du responsable du traitement initial, elle travaille de toute façon sous son contrôle, sous sa surveillance et sous ses instructions, conformément à l'article 16 de la LVP et il ne peut donc pas être question d'indépendance. Dans les termes de la LVP, un sous-traitant n'est pas un tiers vis-à-vis du responsable du traitement (voir article 1, § 6 de la LVP). Vu sous cet angle, l'OI, au sens de l'arrêté royal, n'est pas toujours un maillon indépendant, tant à l'égard de l'expéditeur (responsable du traitement initial) qu'à l'égard du destinataire (responsable du traitement ultérieur).

23. Quant à la thèse formulée au point b.[20], il est en effet exact que l'article 10 de l'arrêté royal du 13 février 2001 – du moins une interprétation littérale de cet article – ne fait aucune distinction selon que les données des différents fournisseurs concernent différentes personnes physiques ou les mêmes personnes physiques.

[20] Voir Vandendriessche, J. : "De verwerking van persoonsgegevens voor historische, statistische en wetenschappelijke doeleinden", *Tijdschrift voor Belgisch burgerlijk recht*, 2006, p. 541 et 543 : "Cette intervention obligatoire (d'une OI, ndlr) est justifiée dans le Rapport au Roi par le danger particulier pour la vie privée qui découlerait de la fusion de différents fichiers de données. Cet argument ne convainc que partiellement. Il existe indubitablement un danger si le responsable du traitement collecte des données à caractère personnel sur les mêmes personnes concernées auprès de plusieurs autres entités, créant ainsi un fichier "plus riche". Le raisonnement ne tient pas tout à fait debout si le responsable du traitement collecte des données à caractère personnel sur différentes personnes concernées auprès de différentes entités. La nature du fichier de données n'en est pas modifiée. Il y a juste un plus gros fichier de données." [Traduction libre réalisée par le secrétariat de la Commission, en l'absence d'une traduction officielle]

24. La Commission estime toutefois que l'interprétation selon laquelle l'article 10 de l'arrêté royal du 13 février 2001 vise également la situation où le responsable du traitement ultérieur veut collecter des données à caractère personnel auprès de différentes entités sur différentes personnes concernées ne tient pas compte de la finalité concrète de l'intervention obligatoire d'une OI. Cette obligation s'explique notamment en raison du risque que les données relatives aux mêmes personnes concernées, provenant de différents fournisseurs, soient agrégées pour être associées et couplées entre elles sur place. L'OI dispose ainsi de plus de données de la personne concernée que chaque fournisseur de données. Un tel fichier "enrichi" leur permet également d'établir des liens éventuels entre les diverses données à caractère personnel.

Ce risque n'est toutefois pas présent si le responsable du traitement ultérieur veut collecter des données à caractère personnel sur plusieurs personnes concernées auprès de plusieurs entités. En outre, cette vision implique que la fusion de deux petits fichiers contenant des données à caractère personnel est ainsi évaluée de manière plus stricte que la communication d'une banque de données beaucoup plus grande, mais identique pour le reste, par un seul responsable du traitement [21] . La Commission part donc du principe que l'article 10 de l'arrêté royal du 13 février 2001 ne vise que la situation spécifique où le responsable du traitement ultérieur veut collecter des données à caractère personnel sur les mêmes personnes concernées auprès de plusieurs entités. Seulement dans ce cas, des données sont en effet couplées, créant ainsi de nouvelles données (enrichies) concernant cette personne.

ii. Un TTP qui code des données et qui intervient en dehors du contexte du Chapitre II de l'arrêté royal du 13 février 2001

25. L'intervention d'un TTP est également envisageable pour le codage de données en dehors du contexte d'un traitement ultérieur à des fins HSS. À cet égard, on peut faire référence aux cas où les données ont déjà été initialement collectées pour des finalités de recherche ou à des situations où le TTP agit dans le cadre d'un traitement ultérieur qui est compatible avec la finalité initiale.

26. Dans ces cas, le Chapitre II de l'arrêté royal du 13 février 2001 n'est pas d'application. Les exigences particulières de ce Chapitre II ne se rapportent en effet qu'aux situations où l'on souhaite effectuer un traitement ultérieur à des fins HSS qui, en soi, est incompatible avec la finalité pour laquelle les données ont été traitées initialement. Si par contre le traitement ultérieur à des fins HSS est compatible avec la finalité initiale, par exemple parce qu'il est autorisé ou imposé par une

[21] Voir Vandendriessche, J., *op. cit.*, p. 543.

disposition légale ou réglementaire[22], les garanties supplémentaires dont il est question dans le Chapitre II de l'arrêté royal du 13 février 2001 ne doivent en principe pas être respectées[23].

27. La compatibilité d'un traitement ultérieur avec la finalité initiale ne porte toutefois pas préjudice aux autres obligations en vertu de la LVP, ni aux autres chapitres de l'arrêté royal du 13 février 2001 :

- ainsi, la logique suivie dans le Chapitre II de l'arrêté royal du 13 février 2001 concernant l'obligation de préférer le traitement de données anonymes ou codées au traitement de données non codées[24] peut également être utilisée dans ces cas, en appliquant le principe de proportionnalité (article 4, § 1, 3° de la LVP) qui requiert que l'on ne peut pas traiter (dans ce cas, communiquer) plus de données que ne le nécessitent les finalités envisagées (et dont on peut déduire que leur degré d'identification ne peut donc pas non plus être excessif) ;

- l'intervention d'un TTP n'est certes pas toujours obligatoire mais est toutefois recommandée à la lumière de l'article 16, § 4 de la LVP lorsque des données, provenant de différentes sources, – relatives aux mêmes personnes concernées – doivent être codées ;

- un traitement de données doit également toujours se dérouler de manière loyale (article 4, § 1, 1° de la LVP) et bien sécurisée (article 4, § 4 de la LVP). Dans cette optique, la Commission insiste pour que le cas échéant, des mesures organisationnelles soient au moins prises afin que le codage de données – provenant de différentes sources et relatives aux

---

[22] Ce constat découle de l'interprétation de l'article 4, § 1, 2° de la LVP. Cet article stipule que "*les données à caractère personnel ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment (…) des dispositions légales et réglementaires applicables.*" La Commission en a déduit qu'un traitement, sur la base de dispositions légales ou réglementaires, peut être considéré comme un traitement autorisé et compatible auquel les dispositions relatives au traitement ultérieur fixées dans l'arrêté d'exécution de la LVP ne s'appliquent pas (voir également dans ce sens l'avis n° 14/2002 du 8 avril 2002). Voir également le Rapport au Roi de l'arrêté royal (p. 7847) : "*Une finalité compatible est dès lors une finalité (…) qu'une disposition légale considère comme compatible.*" Un traitement ultérieur à des fins HSS résultant de dispositions légales ou réglementaires est donc en soi conforme à l'article 4, § 1, 2°, première phrase de la LVP. Les exigences particulières du Chapitre II de l'arrêté royal ne concernent donc que les cas où on souhaite recourir à l'article 4, § 1, 2°, deuxième phrase de la LVP (la 'non-compatibilité' des fins HSS) pour mettre sur pied un traitement qui ne pourrait pas être réalisé sans cela.

[23] Voir le texte du Rapport au Roi de l'arrêté royal (p. 7847) : "*Lorsque des données sont collectées initialement à des fins historiques, statistiques ou scientifiques, ou lorsque la réutilisation de ces données à de telles fins n'est pas incompatible avec la finalité initiale, indépendamment de l'existence de garanties suffisantes, le régime de ces traitements s'avère dans ce cas être le régime ordinaire des traitements de données personnelles.*"

[24] L'article 1 de l'arrêté royal du 13 février 2001, qui fixe les définitions des notions de "*données codées*" et de "*données non codées*", s'applique d'ailleurs intégralement dans ces situations.

mêmes personnes concernées – soit effectué par une unité qui soit distincte du service effectuant la recherche ;

- l'information spécifique prévue pour le traitement ultérieur de données sensibles, judiciaires et relatives à la santé[25] ne s'applique pas dans ce contexte, mais il faut par ailleurs respecter l'article 26 de l'arrêté royal du 13 février 2001, en vertu duquel les raisons de ce traitement doivent être communiquées au préalable aux personnes concernées, ainsi que la liste des catégories de personnes qui ont accès à ces données.

28. Le fait que le Chapitre II de l'arrêté royal du 13 février 2001 ne s'applique pas dans ce cas a donc dans la pratique des conséquences plutôt limitées, étant donné que le TTP doit *de facto* respecter de très nombreuses obligations dudit chapitre. Sur le plan de la déclaration du traitement de données auprès de la Commission, il y a toutefois des différences significatives :

- aucune déclaration ne doit être effectuée pour un traitement *ultérieur* ;
- il suffit d'une déclaration ordinaire qui, le cas échéant – lorsque des données sensibles ou judiciaires sont traitées –, est complétée par les informations visées à l'article 25, 4° de l'arrêté royal du 13 février 2001[26].

29. De plus, dans ce contexte, la Commission attire encore l'attention sur les mêmes points importants tels qu'exposés ci-dessus au point 20 (qui s'appliquent évidemment, outre les conditions générales expliquées au titre IV de la présente recommandation).

iii. Remarque finale : recommandation de la Commission concernant la préférence de l'intervention d'un TTP lors du codage de données

30. Il a déjà été observé ci-dessus que l'intervention d'une OI n'était obligatoire que dans un certain nombre de cas en vertu de l'arrêté royal du 13 février 2001. Ce raisonnement a été appliqué à l'égard des TTP qui codent des données mais qui ne sont pas des OI au sens de l'arrêté royal (cf. le point 27, deuxième flèche). Un critère important pour déterminer si l'intervention d'un TTP est obligatoire/recommandée est de savoir si des données – relatives aux mêmes personnes concernées – provenant de différentes sources sont regroupées, ou s'il n'y a qu'une seule source.
La Commission souhaite toutefois encore ajouter à cela une ligne directrice : dans des situations où des données doivent encore pouvoir être décodées par la suite, elle recommande que le codage –

---

[25] Articles 14 et suivants de l'arrêté royal du 13 février 2001 (cf. le point 19 ci-dessus).

[26] "*lorsque l'information, due en vertu de l'article 9 de la loi, est communiquée à la personne concernée ou lors de la déclaration visée a l'article 17, § 1er, de la loi, le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement de données à caractère personnel visées aux articles 6 à 8 de la loi*.".

que les données proviennent d'une ou de plusieurs sources – soit effectué par un TTP (une OI) et pas par la (les) source(s) de données initiale(s). Une intervention d'un TTP offre en effet dans de telles situations des garanties supplémentaires pour éviter des décodages interdits.

D. Conditions supplémentaires pour les TTP qui agrègent des données (cf. le titre III, point C de la présente recommandation)

31. Le TTP doit utiliser tous les moyens techniques afin de rendre impossible une identification des personnes concernées par le responsable du traitement (ultérieur). Il doit donc agréger les données à caractère personnel à un niveau suffisamment élevé. La Commission estime par exemple que les résultats communiqués par le TTP ne peuvent en principe pas contenir de groupes comportant moins de trois éléments.

32. À titre d'exemple : supposons que le TTP, dans l'exemple susmentionné (cf. le point 11 ci-dessus), constate qu'en 2008, on n'a recensé qu'une seule personne de 21 ans atteinte d'un cancer du poumon, il faut alors s'efforcer de communiquer ce résultat au chercheur à un niveau d'agrégation plus élevé, en mentionnant par exemple uniquement que dans la catégorie d'âge entre 20 et 25 ans, dix cas ont été constatés. La communication de résultats pour l'âge exact de 21 ans impliquerait en effet dans ce cas des risques importants de réidentification.

V. UN TTP EST-IL UN SOUS-TRAITANT OU UN RESPONSABLE DU TRAITEMENT ?

33. Pour les cas visés au Chapitre II de l'arrêté royal du 13 février 2001 (OI), la question de savoir si un TTP agit en tant que responsable du traitement ou en tant que sous-traitant au sens de la LVP est explicitement mentionnée dans ledit arrêté royal (à savoir, soit en tant que sous-traitant du fournisseur unique de données, soit en tant que responsable du traitement dans le cas de plusieurs fournisseurs de données), alors que cette question ne peut pas toujours être posée avec certitude dans toutes les autres situations mentionnées sous le titre III de la présente recommandation. En la matière, la Commission donne les lignes directrices suivantes :

- lorsque des données à caractère personnel des mêmes personnes concernées sont réclamées auprès de différents fournisseurs de données et qu'elles sont regroupées par le TTP avant d'être couplées, cela engendre une certaine menace pour la protection de la vie privée. Cela requiert dès lors qu'un TTP offre des garanties adéquates.

  C'est pourquoi la Commission estime que dans de pareils cas, le TTP ne peut pas intervenir en tant que simple sous-traitant, mais doit pouvoir être interpellé de manière autonome en

tant que responsable distinct du traitement, et ce spécifiquement pour les traitements qu'il exécute ;

- dans d'autres situations aussi, le TTP pourra souvent être qualifié de responsable du traitement. Ce sera notamment le cas si le TTP est un des rares acteurs sur le marché qui peut fournir un service particulier et si la structure du réseau qu'il installe implique que le traitement de données se fait nécessairement d'une manière déterminée (sans que les responsables des traitements initial et ultérieur n'aient voix au chapitre en la matière). À titre d'exemple, on peut ici penser à la Banque-carrefour de la Sécurité sociale ;

- la Commission précise enfin que lorsque les finalités et les moyens des traitements de données effectués ont un cadre réglementaire, le responsable du traitement doit être désigné par le législateur (article 1, § 4 de la LVP).

VI. TTP ET INTÉGRATEURS DANS LE SECTEUR PUBLIC

34. La Commission rappelle sa recommandation en matière d'intégrateurs dans le secteur public. Elle est consciente du fait que le rôle d'un TTP et celui d'un intégrateur dans le secteur public coïncideront parfois.

35. Elle envisage donc le rapport entre les deux concepts comme suit : les intégrateurs de services et de données dans le secteur public – s'ils remplissent les conditions de la recommandation n° 03/2009 du 1er juillet 2009 – pourront également intervenir en tant que TTP[27]. En principe, ils pourront – dans leur propre sphère de compétence – remplir le rôle de toutes les fonctions de TTP énumérés sous le titre III de la présente recommandation.

36. Toutefois, l'inverse n'est pas valable : un TTP ne sera pas toujours un intégrateur au sens de la recommandation n° 03/2009. En effet, il existe une différence essentielle entre les deux : les TTP ne doivent pas toujours être autorisés par ou en vertu d'une loi pour pouvoir remplir leur rôle. Pour l'intégration de services au sein du secteur public, un tel mandat légal est toutefois indispensable. Il faut en effet constater que les intégrateurs de services existants[28] sont (ou seront) tous repris dans un cadre légal ou décrétal strict.

---

[27] Dans la recommandation n° 03/2009 (point 34), la Commission a mis l'accent sur le fait que le champ d'action d'un intégrateur de services doit être clairement délimité afin d'éviter le chevauchement des champs d'action d'intégrateurs de services.

[28] Par exemple la Banque-carrefour de la sécurité sociale, la plate-forme eHealth, Fedict.

37. Toutes les fonctions de TTP énumérées sous le titre III de la présente recommandation peuvent donc en principe également être exercées par des institutions privées, en particulier celles mentionnées aux points A à C inclus. Toutefois, dans ce cadre, d'importantes limitations concernant les données communiquées à ou par des instances publiques sont d'application. Les TTP qui interviennent aujourd'hui dans des secteurs publics où l'échange de données est réglementé par une législation spéciale sont par exemple toutes des institutions publiques. À titre d'exemple, on peut signaler l'article 14 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en vertu duquel toute communication de données sociales à caractère personnel pour ou à des institutions de sécurité sociale doit en principe se faire à l'intervention de la Banque-carrefour de la sécurité sociale. Il est dès lors impensable que dans ce domaine, la fonction de TTP soit exercée par une entreprise privée[29].

VII. REMARQUE FINALE : PORTÉE DE LA PRÉSENTE RECOMMANDATION

38. Il a été précisé ci-dessus que la Commission reconnaissait que dans un certain nombre de cas, l'intervention d'un TTP peut signifier une plus-value pour protéger la vie privée des personnes concernées lors d'échanges de données. Dans ce contexte, elle donne plusieurs lignes directrices, ainsi que certaines indications concernant la manière dont elle interprète certaines règles de l'arrêté royal du 13 février 2001.

39. Toutefois, elle est bien consciente du fait que dans la pratique, on peut envisager des situations et des échanges de données très divergents pour lesquels un TTP peut jouer un rôle. Dans cette optique, elle se réserve toujours le droit d'évaluer dans des cas concrets la compatibilité des modalités de création d'un nouveau TTP (ou d'utilisation d'un TTP existant) avec les principes de protection de la vie privée.

Pour l'Administrateur e.c., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere

[29] À moins que, le cas échéant, en tant que sous-traitant, pour le compte de l'institution qui exerce la fonction de TTP.