

Avis du contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative aux normes de qualité et de sécurité des organes humains destinés à la transplantation

(2009/C 192/02)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité instituant la Communauté européenne, et notamment son article 286,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, et notamment son article 41,

vu la demande d'avis formulée conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001, transmise au CEPD le 8 décembre 2008,

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

Proposition de directive relative aux normes de qualité et de sécurité des organes humains destinés à la transplantation

1. Le 8 décembre 2008, la Commission a adopté une proposition de directive du Parlement européen et du Conseil relative aux normes de qualité et de sécurité des organes humains destinés à la transplantation (ci-après dénommée «la proposition») ⁽¹⁾. Elle a transmis cette proposition au CEPD pour consultation, conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001.

2. La proposition vise à garantir des normes de qualité et de sécurité élevées pour les organes humains destinés à la transplantation, afin d'assurer un niveau élevé de protection de la santé humaine. En particulier, la proposition:

- précise les exigences fondamentales de qualité et de sécurité que doivent comprendre les systèmes de transplantation des États membres et prévoit la création ou la désignation d'une autorité nationale compétente chargée de veiller au respect de ces exigences. À cette fin, des programmes nationaux de qualité relatifs à l'obtention et au transfert d'organes humains seront établis dans tous les pays et comprendront notamment un système de notification des incidents ou des réactions

indésirables graves, ainsi qu'un mécanisme de traçabilité visant à garantir que tous les organes soient traçables du don à la réception et inversement;

- assure la protection des donneurs et des receveurs. En ce qui concerne les donneurs vivants en particulier, la proposition comporte des mesures relatives à l'évaluation de leur état de santé, à leur information exhaustive concernant les risques avant le don et à l'introduction de *registres des donneurs vivants*, ainsi que des mesures visant à garantir le caractère altruiste et volontaire des dons d'organes effectués par des donneurs vivants;

- facilite la coopération entre les États membres et les *échanges transfrontaliers d'organes* (également entre des États membres et des pays tiers), en établissant des procédures normalisées pour la collecte des informations pertinentes concernant les caractéristiques de l'organe, ainsi qu'un mécanisme pour la transmission des informations.

3. La mise en œuvre du système proposé pour les dons et les transplantations implique le traitement de données à caractère personnel relatives à l'état de santé des donneurs et des receveurs d'organes par des organismes agréés et des professionnels du monde de la santé dans les différents États membres. Ces données, considérées comme sensibles, sont soumises aux règles plus strictes en matière de protection des données prévues à l'article 8 de la directive 95/46/CE, relatif aux catégories particulières de données.

4. Plus précisément, les données relatives aux donneurs sont traitées par les organismes d'obtention, qui rassemblent les informations sur les caractéristiques du donneur et de l'organe et déterminent ainsi si l'organe concerné convient pour une transplantation (une liste de ces données figure en annexe de la proposition). Les données relatives aux receveurs (patients) sont traitées dans les centres de transplantation dans lesquels l'opération se déroule effectivement. Même si les données relatives au donneur ne sont pas communiquées au patient (et inversement), les autorités nationales compétentes sont néanmoins tenues d'assurer en permanence la traçabilité complète de l'organe du donneur au receveur (et inversement), ce qui devrait également être possible lors d'échanges transfrontaliers d'organes.

Consultation du CEPD

5. Le CEPD se félicite d'être consulté sur cette question conformément à l'article 28 du règlement (CE) n° 45/2001 et relève avec satisfaction qu'il est fait référence à cette consultation dans le préambule de la proposition.

⁽¹⁾ Doc. COM(2008) 818 final.

6. La proposition fera progresser les procédures en vigueur en matière de don et de transplantation d'organes, l'objectif in fine étant d'augmenter la disponibilité d'organes et de réduire le taux de mortalité des demandeurs d'organes se trouvant sur des listes d'attente. Elle complète le cadre législatif existant en ce qui concerne l'utilisation de matériel biologique d'origine humaine⁽¹⁾. En outre, elle peut être considérée comme s'inscrivant dans le cadre de l'approche globale de la CE visant à fixer différents types de normes communes pour la prestation de services de soins de santé dans les États membres, afin, essentiellement, de promouvoir la disponibilité transfrontière de ces services dans toute l'Europe⁽²⁾. Le CEPD est favorable à ce type d'approche, comme il l'a déjà indiqué dans son avis sur les droits des patients en matière de soins de santé transfrontaliers. Toutefois, il insiste à nouveau sur la nécessité d'adopter un point de vue bien coordonné et uniforme en matière de protection des données dans les différentes initiatives liées aux soins de santé⁽³⁾.
7. La proposition a déjà pris en compte les besoins en matière de protection des données tant pour les donneurs que pour les receveurs d'organes. L'élément le plus important est l'obligation de préserver le caractère confidentiel de l'identité des donneurs et des receveurs (considérants 11 et 16, articles 10 et 17). Quelques références générales à la protection des données figurent en outre dans certaines parties du texte de la proposition [considérant 17, article 16, article 4, paragraphe 3, point a), article 15, paragraphe 3, article 19, paragraphe 1, point a), et l'annexe], qui mentionne aussi plus spécifiquement la nécessité de coopérer avec les autorités nationales compétentes en matière de protection de données [article 18, point f), et article 20, paragraphe 2].
8. Le CEPD se déclare satisfait du contenu des dispositions susmentionnées. Il souhaite néanmoins faire part de ses préoccupations à propos de certaines dispositions qui ne sont pas suffisamment précises ou explicites et qui, étant une source d'ambiguïtés, risqueraient de compromettre la mise en œuvre uniforme de la proposition par les États membres.
9. Plus précisément, l'utilisation parfois contradictoire des concepts de «traçabilité des organes» et d'«anonymat des donneurs et des receveurs» est une question qui mérite des clarifications et des précisions supplémentaires. Dans cet ordre d'idée, il conviendrait d'insister davantage pour que des mesures de sécurité renforcées en termes de protection des données relatives aux donneurs et aux receveurs soient adoptées au niveau des États membres, afin d'assurer un niveau de protection des données plus élevé dans les différents pays européens et de garantir le respect de la protection des données lors d'échanges transfrontières d'organes (que ce soit entre pays européens ou avec des pays tiers).

⁽¹⁾ Ce cadre comprend les directives 2002/98/CE, 2004/33/CE, 2005/61/CE et 2005/62/CE pour le sang et les produits sanguins et les directives 2004/23/CE, 2006/17/CE et 2006/86/CE pour les cellules et les tissus humains.

⁽²⁾ Voir aussi la proposition de directive du Parlement européen et du Conseil relative à l'application des droits des patients en matière de soins de santé transfrontaliers, COM(2008) 414 final.

⁽³⁾ Avis du CEPD du 2 décembre 2008 sur la proposition de directive relative à l'application des droits des patients en matière de soins de santé transfrontaliers.

10. Le présent avis apportera des précisions sur les questions susmentionnées, le but étant d'améliorer le contenu des dispositions relatives à la protection des données qui figurent actuellement dans la proposition, en termes tant de clarté que de cohérence.

II. CLARIFICATION DES NOTIONS DE TRAÇABILITÉ ET D'ANONYMAT

Applicabilité de la directive 95/46/CE

11. Aux termes de l'article 2, point a), de la directive 95/46/CE sur la protection des données à caractère personnel, on entend par «données à caractère personnel»: «toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale».
12. Le matériel biologique d'origine humaine, tels que les organes, les tissus, les cellules ou le sang, peut être défini comme du matériel pouvant être prélevé sur le corps humain. On peut se demander si ce matériel peut être considéré en tant que tel comme des données à caractère personnel; ce qui est incontestable, en revanche, c'est qu'il peut être utilisé comme une *source* d'informations à caractère personnel sur les personnes concernées. L'extraction de ces informations constitue souvent la finalité du traitement de matériel biologique et, même en l'absence de cette finalité, le matériel biologique est généralement accompagné des informations ainsi obtenues. Dans ces conditions, les règles énoncées dans la directive 95/46/CE s'appliquent⁽⁴⁾ pour autant que la personne concernée soit une personne (physique) *identifiée* ou *identifiable*.
13. Le considérant 26 de la directive 95/46/CE explique comment déterminer si une personne est identifiable: «il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne». Le même considérant explique ensuite que les règles de la directive ne s'appliquent pas si les informations se rapportent à une personne qui n'est pas ou n'est plus identifiable: ces données sont alors considérées comme *anonymes*.
14. Dans sa recommandation (2006) 4, le Conseil de l'Europe a traité de la question spécifique du caractère identifiable du matériel biologique, en établissant une distinction entre le matériel biologique identifiable et non identifiable⁽⁵⁾.
15. Selon cette recommandation, le matériel biologique identifiable «correspond à du matériel biologique qui, seul ou combiné à des données associées, permet d'identifier la personne concernée soit directement, soit au moyen d'un code»⁽⁶⁾. Dans le dernier cas, l'utilisateur du matériel

⁽⁴⁾ Groupe de travail «article 29» sur la protection des données, avis n° 4/2007 sur le concept de données à caractère personnel, p. 9.

⁽⁵⁾ Recommandation Rec(2006) 4 du Comité des ministres aux États membres sur la recherche utilisant du matériel biologique d'origine humaine.

⁽⁶⁾ Article 3, point i), de la recommandation Rec(2006) 4.

biologique peut, soit avoir accès au code («matériel codé»), soit ne pas y avoir accès, le code étant placé sous le contrôle d'un tiers («matériel rendu anonyme de façon réversible»). Dans son avis n° 4/2007 sur le concept de données à caractère personnel, le groupe de l'article 29 a utilisé la notion de *données pseudonymisées de manière retraçable* pour désigner des informations permettant l'identification indirecte de personnes physiques, données qui peuvent être toujours être utilisées pour établir une correspondance avec une personne et l'identifier dans des cas spécifiques définis à l'avance⁽¹⁾. Les *données codées* sont citées à titre d'exemple où des données à caractère personnel correspondent à un code, la clé qui permet d'établir une correspondance entre ce code et des identifiants courants de ces personnes physiques étant conservée séparément. Si les codes attribués sont uniques et correspondent à une personne spécifique, l'identification est possible à condition d'avoir accès à la clé d'encryptage utilisée.

16. La recommandation fait également référence au *matériel biologique non identifiable* (ou «matériel biologique rendu anonyme de façon irréversible»). Cette expression désigne le «matériel biologique qui, seul ou combiné à des données associées, ne permet pas, moyennant des efforts raisonnables, d'identifier la personne concernée»⁽²⁾. Ces données devraient en fait être considérées comme des données anonymes au sens de la directive 95/46/CE.
17. Il ressort de ce qui précède que la directive 95/46/CE s'applique à la collecte, au stockage et au traitement des organes identifiables et à l'extraction qui s'ensuit des informations obtenues à partir de ces organes, aussi longtemps que celle-ci demeure possible en tenant dûment compte de tous les moyens pouvant raisonnablement être mis en œuvre pour identifier la personne concernée. Comme on le verra plus loin, la traçabilité permanente des organes, telle qu'elle est envisagée dans la directive proposée, implique que les personnes demeurent identifiables tout au long du processus.

Traçabilité ou caractère anonyme des organes humains

18. La traçabilité d'un matériel biologique est la possibilité de remonter aux diverses personnes concernées et, par conséquent, d'identifier celles-ci. En d'autres termes, chaque fois qu'il est possible de retrouver, d'une manière directe ou indirecte, les personnes concernées par un transfert de matériel biologique, ces dernières peuvent être considérées comme identifiables — et inversement. Les concepts de «traçabilité» et de «possibilité d'identification» sont par conséquent étroitement liés par principe. En revanche, la traçabilité et l'anonymat des données sont incompatibles simultanément: ces concepts s'excluent mutuellement. Si certaines informations sont vraiment anonymes, il n'est pas possible d'identifier et de retrouver les personnes concernées.
19. Dans le contexte de la proposition actuelle, la traçabilité est une obligation impérative qui doit être transposée dans les programmes nationaux de qualité des États membres à deux égards: celui des donneurs et celui des receveurs. Par conséquent, même si les informations relatives aux donneurs et aux receveurs demeurent confidentielles,

celles qui concernent les organes permettent, en revanche, une identification. C'est également ce qui ressort de la définition de la traçabilité énoncée à l'article 3 de la proposition: «la capacité d'une autorité compétente à localiser et à identifier l'organe à chaque étape de la chaîne qui va du don à la transplantation ou à l'élimination, cette autorité étant autorisée, dans les circonstances spécifiques précisées dans la présente directive à identifier le donneur et l'organisme d'obtention, à identifier le ou les receveurs dans le ou les centres de transplantation, à localiser et à identifier toutes les informations non personnelles pertinentes concernant les produits et les matériels entrant en contact avec cet organe».

20. En outre, l'article 10 de la proposition, qui porte sur la traçabilité, précise dans son premier paragraphe que «les États membres veillent à ce que tous les organes obtenus et attribués sur leur territoire fassent l'objet d'une traçabilité du donneur au receveur et inversement, de manière à protéger la santé des donneurs et des receveurs». Le paragraphe 3 du même article est libellé comme suit: «Les États membres font en sorte: a) que l'autorité compétente ou les autres organismes intervenant dans la chaîne qui va du don à la transplantation ou à l'élimination conservent les données nécessaires pour assurer la traçabilité à toutes les étapes de ladite chaîne conformément au programme national de qualité; b) que les données requises pour assurer une traçabilité complète soient conservées pendant au moins trente ans après le don. Ces données peuvent être stockées sous forme électronique».
21. Le processus de traçabilité devra encore faire l'objet de mesures d'application (article 25 de la proposition), mais il semble bien que l'on s'oriente vers un système permettant l'identification indirecte des donneurs et des receveurs, établi sur la base de la directive 2004/23/CE⁽³⁾ relative aux tissus ou cellules humains et du code d'identification européen qui y est prévu⁽⁴⁾, ou, du moins, vers un système qui assurera une interopérabilité avec cette directive. Dans

⁽³⁾ Étant donné que les donneurs d'organes sont généralement aussi des donneurs de tissus, il faut pouvoir également retracer et consigner toute réaction négative imprévue dans le système de surveillance des tissus, et, par conséquent, veiller à l'interopérabilité avec la méthode d'identification indirecte utilisée dans ce système. Voir la directive 2004/23/CE du Parlement européen et du Conseil du 31 mars 2004 relative à l'établissement de normes de qualité et de sécurité pour le don, l'obtention, le contrôle, la transformation, la conservation, le stockage et la distribution des tissus et cellules humains (JO L 102/48 du 7.4.2004), et la directive de la Commission 2006/86/CE du 24 octobre 2006 portant application de la directive 2004/23/CE du Parlement européen et du Conseil en ce qui concerne les exigences de traçabilité, la notification des réactions et incidents indésirables graves, ainsi que certaines exigences techniques relatives à la codification, à la transformation, à la conservation, au stockage et à la distribution des tissus et cellules d'origine humaine (JO L 294/32 du 25.10.2006).

⁽⁴⁾ Ce code comprend un numéro d'identification unique pour chaque don qui, en combinaison avec l'établissement de tissus et l'identification du produit, permet de remonter jusqu'aux donneurs et aux receveurs. Plus précisément, selon l'article 10 de la directive 2006/86/CE, «un code d'identification européen unique est attribué à tous les produits de l'établissement de tissus et cellules, quels qu'ils soient, afin de garantir une identification adéquate du donneur et la traçabilité de tous les produits de l'établissement de tissus et cellules et de fournir des informations sur les principales caractéristiques et propriétés des tissus et des cellules». Comme précisé à l'annexe VII de cette directive, le code comprend deux parties: a) l'identification du don, notamment un numéro d'identification unique attribué au don et l'identification de l'établissement de tissus; et b) l'identification du produit, qui inclut le code du produit, le numéro du sous-lot et la date d'expiration.

⁽¹⁾ Groupe article 29 sur la protection des données, avis n° 4/2007, p. 18.

⁽²⁾ Article 3, point ii), de la recommandation Rec(2006) 4.

cette éventualité, le traitement des données relatives aux donneurs et aux receveurs visé dans la proposition concernerait le matériel biologique rendu anonyme de façon réversible, dénommé «données pseudonymisées de manière retraçable» dans la terminologie propre à la protection des données (voir ci-dessus, au point 15), données auxquelles les dispositions de la directive 95/46/CE seraient dès lors applicables.

22. Il convient toutefois de noter que, malgré les obligations claires qui sont fixées en matière de traçabilité et d'identification, les termes d'«anonymat» ou de «données anonymes» sont utilisés dans certaines parties du texte de la proposition pour qualifier les données relatives aux donneurs et aux receveurs — ce qui comme expliqué ci-dessus, est contradictoire et prête fortement à confusion ⁽¹⁾.
23. Plus spécifiquement, le paragraphe 2 de l'article 10 de la proposition, qui établit la nécessité de prévoir un système permettant l'identification du donneur, est libellé comme suit: «Les États membres veillent à la mise en œuvre d'un système d'identification des donneurs permettant d'identifier chaque don et chacun des organes qui lui sont associés. Ils veillent à ce que ce système d'identification des donneurs soit conçu et choisi en conformité avec l'objectif visant à ne pas collecter, traiter ou utiliser de données à caractère personnel ou à en collecter, traiter ou utiliser le moins possible. Il convient en particulier d'utiliser les possibilités de pseudonymisation ou d'anonymisation» ⁽²⁾. Le CEPD estime que les termes soulignés dans ce paragraphe sont incompatibles avec le concept de traçabilité, puisqu'il est impossible que les données soient traçables et identifiables lorsque les donneurs et les receveurs sont rendus anonymes. De plus, il est curieux de constater que ce paragraphe fait référence à l'identification du donneur et qu'il n'y est nullement fait mention de l'identification du receveur (qui est également concerné par le processus de transplantation).
24. La contradiction dont il est question ci-dessus est encore plus évidente à l'article 17, qui porte sur l'anonymat des donneurs et des receveurs: «Les États membres prennent toutes les mesures nécessaires pour garantir l'anonymisation de toutes les données à caractère personnel des donneurs et des receveurs traitées dans le cadre de la présente directive, dans le but de prévenir l'identification tant des donneurs que des receveurs». Cet article est en totale contradiction avec les articles de la proposition relatifs à la traçabilité.

Confidentialité plutôt qu'anonymat

25. Le CEPD croit comprendre que le terme «anonymat» est en fait utilisé pour souligner la nécessité de renforcer la *confidentialité* ⁽³⁾ des données relatives aux donneurs et aux rece-

veurs, c'est-à-dire pour s'assurer que les informations ne soient accessibles qu'aux personnes qui sont autorisées à y avoir accès. Il présume que le terme d'anonymisation est plus spécifiquement utilisé pour désigner un système permettant l'identification indirecte des donneurs et des receveurs ⁽⁴⁾, ce qui peut également être déduit de la manière dont ce terme est utilisé dans la directive 2004/23/CE relative aux tissus et cellules humains. Toutefois, comme nous l'avons dit plus haut, le terme «anonymat» n'est pas celui qu'il convient d'utiliser.

26. Le protocole additionnel à la convention sur les droits de l'homme et la biomédecine ⁽⁵⁾ du Conseil de l'Europe illustre la manière dont la protection des données et la traçabilité peuvent être envisagés conjointement dans le cadre d'un processus de transplantation. Ce protocole utilise le concept de confidentialité et non celui d'anonymat. Ainsi, son article 23, paragraphe 1, indique que «toutes les données à caractère personnel concernant la personne sur laquelle a été pratiqué le prélèvement d'organes ou de tissus ainsi que les données concernant le receveur doivent être considérées comme confidentielles. Elles ne peuvent être collectées, traitées et communiquées que dans le respect des règles relatives au secret professionnel et à la protection des données à caractère personnel». Le paragraphe 2 ajoute que: «les dispositions du paragraphe précédent s'entendent sans préjudice des dispositions permettant, sous réserve de garanties appropriées, la collecte, le traitement et la communication des informations nécessaires sur la personne sur laquelle a été pratiqué le prélèvement ou sur le(s) receveur(s) d'organes ou de tissus lorsque des raisons médicales l'exigent, y compris la traçabilité, conformément à l'article 3 du présent protocole».
27. Compte tenu de ce qui précède, le CEPD recommande d'adapter la terminologie utilisée dans certaines parties de la proposition pour éviter les ambiguïtés et d'indiquer de manière explicite que les données ne sont pas anonymes, mais qu'il convient de procéder à leur traitement en respectant des règles strictes en matière de confidentialité et de sécurité. Plus précisément, il recommande d'apporter les modifications suivantes:

⁽⁴⁾ Selon le contexte dans lequel il est utilisé, le terme anonymisation désigne parfois des données qui permettent l'identification indirecte, comme dans le domaine des statistiques, par exemple. Cette acception n'est toutefois pas pertinente du point de vue de la protection des données, comme le CEPD l'a expliqué dans son avis sur la proposition de règlement du Parlement européen et du Conseil relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail [COM(2007) 46 final] et sur la proposition de règlement du Parlement européen et du Conseil relatif aux statistiques européennes [COM(2007) 625 final].

⁽⁵⁾ Conseil de l'Europe, Protocole additionnel à la convention sur les droits de l'homme et la biomédecine relatif à la transplantation d'organes et de tissus d'origine humaine, Strasbourg, le 24.1.2002, voir <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=186&CM=8&DF=2/13/2009&CL=ENG> pour la charte de ratification. Voir également: Conseil de l'Europe, Convention pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine: Convention sur les droits de l'homme et la biomédecine, Oviedo, 4.4.1997, voir <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CM=8&DF=2/13/2009&CL=ENG> pour la charte de ratification.

⁽¹⁾ Le CEPD avait déjà formulé la même observation dans ses commentaires du 19 septembre 2006 sur la consultation publique relative à l'action future de l'UE dans le domaine du don et de la transplantation d'organes.

⁽²⁾ Termes mis en évidence par le CEPD.

⁽³⁾ La confidentialité a été définie par l'Organisation internationale de normalisation (ISO) comme le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé (source: <http://www.wikipedia.org>).

- dernière phrase du considérant 16: «Conformément à cette charte et pour tenir compte comme il se doit de la Convention sur les droits de l'homme et la biomédecine, les programmes de transplantation d'organes doivent reposer sur les principes de don volontaire et non rémunéré, d'altruisme du donneur et de solidarité entre ce dernier et le receveur, tout en veillant à ce que des règles strictes en matière de confidentialité et des mesures de sécurité rigoureuses soient mises en place pour assurer la protection des données à caractère personnel des donneurs et des receveurs»;
 - article 10, paragraphe 2: «Les États membres veillent à la mise en œuvre d'un système d'identification des donneurs et des receveurs permettant d'identifier chaque don et chacun des organes qui lui sont associés. Ils veillent à ce que ce système d'identification des donneurs et des receveurs soit conçu et choisi en conformité avec l'objectif visant à collecter, traiter ou utiliser le moins possible de données à caractère personnel, en recourant notamment aux méthodes de pseudonymisation, et à ce que les mesures techniques et organisationnelles nécessaires soient mises en place pour assurer la sécurité de ces données»;
 - l'article 17 pourrait être supprimé, et son contenu (qui porte sur les besoins en matière de confidentialité) intégré dans un nouveau paragraphe de l'article 16 relatif à la protection des données à caractère personnel, à la confidentialité et à la sécurité du traitement (voir point 36 ci-dessous).
28. Le CEPD propose en outre, comme il s'en expliquera plus loin, de souligner davantage la nécessité de *renforcer la protection* des données relatives aux donneurs et aux receveurs en appliquant des *mesures de sécurité strictes* tant au niveau national qu'au niveau transfrontière.
- III. METTRE L'ACCENT SUR LES MESURES DE SÉCURITÉ NATIONALES À PRENDRE EN MATIÈRE DE PROTECTION DES DONNÉES**
- Besoins et exigences fondamentaux en matière de sécurité*
29. Il ressort de la proposition que le traitement des données à caractère personnel des donneurs et des receveurs se fait principalement au niveau national, c'est-à-dire dans les centres d'obtention et de transplantation des États membres. C'est également à ce niveau que les registres des donneurs vivants sont tenus à jour. Bien que le mécanisme de traçabilité n'ait pas encore été défini, on peut s'attendre à ce que toutes les activités de codification aient également lieu au niveau national, même si c'est un système de codage européen qui va être utilisé, puisque l'identification des donneurs et des receveurs n'est possible que par l'intermédiaire des autorités nationales compétentes.
30. Il est donc de la plus haute importance d'appliquer, au sein des services nationaux compétents, une politique en matière de sécurité des informations qui soit basée sur des *mesures de sécurité strictes et bien conçues*, permettant en particulier de respecter les exigences de confidentialité à l'égard des donneurs et des receveurs qui sont fixées dans la directive et de garantir l'intégrité ⁽¹⁾, la responsabilité ⁽²⁾ et la disponibilité ⁽³⁾ à propos de ces données. À cet égard, la politique en matière de sécurité des informations devrait comprendre des éléments de sécurité physique et logique axés, notamment, sur le contrôle de l'introduction, de l'accès, de l'enregistrement, du transfert et de la communication des données, ainsi que sur le contrôle des supports et du stockage des données.
31. En ce qui concerne la confidentialité, les données médicales des receveurs ⁽⁴⁾, ainsi que les données utilisées pour assurer la caractérisation et le suivi des donneurs [relatives également aux «donneurs marginaux» ⁽⁵⁾], peuvent comporter des informations à caractère personnel sensibles qui sont susceptibles d'affecter la vie sociale, professionnelle et privée des personnes concernées. La protection des données d'identification des donneurs revêt une importance plus grande encore, dans la mesure où les donneurs vivants qui ont consenti au prélèvement d'un ou de plusieurs organes après leur décès pourraient devenir victimes de trafics d'organes et de tissus humains si ces informations venaient à être divulguées. L'intégrité des données relatives aux organes est aussi un élément fondamental, étant donné que la moindre erreur dans les informations transmises pourrait mettre en danger la vie du receveur. Il en va de même pour l'exactitude des données relatives à l'état de santé des donneurs avant la transplantation, puisque ces données sont utilisées afin de déterminer si l'organe concerné convient ou non. S'agissant de la responsabilité, vu le très grand nombre d'organismes différents qui interviennent dans le système global de don et de transplantation, il faudrait trouver un moyen de sensibiliser et responsabiliser toutes les entités concernées, en ce qui concerne notamment les cas où des données d'identification des donneurs seraient communiquées à des personnes non autorisées et/ou les renseignements médicaux relatifs aux organes seraient inexacts. Enfin, étant donné que tout le système repose sur le transfert de données relatives aux
- ⁽¹⁾ Garantir que les données soient «intégrales» ou complètes, c'est-à-dire qu'elles soient conservées sans subir aucune altération au cours de leur traitement éventuel (transfert, stockage ou recherche, par exemple) et maintenues dans un état permettant leur utilisation pour les fins auxquelles elles sont destinées ou, s'agissant de traitements particuliers, à ce qu'elles répondent aux attentes existant a priori en matière de qualité des données. En termes simples, l'intégrité des données est la garantie que les données sont cohérentes et exactes (source: <http://www.wikipedia.org>), que les informations ne sont accessibles qu'aux personnes habilitées à cet effet ou ne peuvent être modifiées que par celles-ci (source: <http://searchdatacenter.techtarget.com>).
- ⁽²⁾ Obligation de répondre de ses actes; non-répudiation: veiller à ce que les données aient été envoyées et reçues par les parties qui disent les avoir effectivement envoyées ou reçues: principe qui garantit qu'une partie à un conflit ne peut réfuter ou mettre en cause la validité d'une déclaration (source: <http://www.wikipedia.org>).
- ⁽³⁾ La mesure dans laquelle il est possible d'avoir un accès instantané aux données (source: <http://www.pcmag.com>).
- ⁽⁴⁾ Il convient de noter que le simple fait d'avoir subi une transplantation d'organe constitue une donnée à caractère personnel sensible concernant l'état de santé du receveur.
- ⁽⁵⁾ Il s'agit de donneurs potentiels, qui n'ont pas le profil idéal, mais qui pourraient entrer en considération dans certaines circonstances, par exemple pour des receveurs âgés. Voir document de travail des services de la Commission accompagnant la proposition de directive du Parlement européen et du Conseil relative aux normes de qualité et de sécurité des organes humains destinés à la transplantation et la communication de la Commission intitulée «Plan d'action sur le don et la transplantation d'organes (2009-2015): renforcement de la coopération entre les États membres — Résumé de l'analyse d'impact», 8.12.2008.

organes et sur le mécanisme de traçabilité du donneur au receveur, il conviendrait que ces données soient mises à la disposition des personnes autorisées, qui pourraient les consulter dès qu'elles en ont besoin et sans devoir attendre (l'indisponibilité des informations compromettrait en effet le bon fonctionnement du système).

32. À cet égard, il faudrait mettre en place des *mécanismes d'autorisation* appropriés, reposant sur des *politiques spécifiques en matière de contrôle d'accès*, qui s'appliquent tant aux bases de données nationales qu'aux échanges transfrontières d'organes. Lesdites politiques devraient, dans un premier temps, être définies au niveau organisationnel, pour ce qui concerne en particulier les procédures d'identification des donneurs et des receveurs (par exemple, qui a accès à quelles informations et dans quelles circonstances). C'est en procédant ainsi que l'on définirait les *droits d'accès*, ainsi que les *scénarios d'accès* dans lesquels ces droits peuvent être exercés (par exemple, les circonstances dans lesquelles l'organisme d'obtention peut communiquer des données à l'autorité compétente et la procédure à suivre à cet effet, les cas — éventuels — dans lesquels l'identité du donneur doit être révélée au receveur et les procédures à suivre à cet effet, etc.). Si l'on veut que ces politiques soient efficaces, il convient que les personnes qui interviennent dans le traitement soient tenues de respecter des *règles spécifiques en matière de confidentialité*.
33. Une fois définies, ces politiques pourront être mises en œuvre sur le plan technique, c'est-à-dire en assurant le contrôle d'accès de l'utilisateur aux systèmes et applications, conformément aux droits d'accès qui auront été prédéfinis. Les technologies ayant fait leurs preuves, telles que l'*encryptage* et les *certificats numériques* ⁽¹⁾ [par exemple, basées sur les *infrastructures à clefs publiques* ⁽²⁾], peuvent être utilisées à cet effet. Des *mécanismes d'identification basés sur le rôle* peuvent aussi être utilisés afin de restreindre les droits d'accès de l'utilisateur en fonction de son rôle (par exemple, afin de prévoir que seuls les médecins seront habilités à modifier les données médicales relatives aux receveurs et aux donneurs qui figurent dans les bases de données nationales).
34. Le contrôle d'accès devrait être complété par des possibilités d'*enregistrer* les actions des utilisateurs (par exemple accès en lecture et en écriture aux données médicales), en particulier lorsqu'il est fait usage de systèmes électroniques. Des mesures relatives à la sécurité physique et logique devraient également être prises afin de garantir que les bases de données relatives aux donneurs et aux receveurs, qui constituent l'élément central du système de don et de transplantation proposé, sont *pleinement opérationnelles*. La disponibilité des données devrait être considérée comme la pierre angulaire du système. À cet égard, la politique en matière de sécurité des informations devrait être fondée sur une *analyse et une évaluation pertinentes du risque* et devrait comporter des éléments tels que la gestion des incidents et de la continuité des activités. Tous ces éléments devraient être préservés et améliorés grâce à des procédures régulières de surveillance et de réexamen. Des *audits indépendants*

peuvent également accroître l'efficacité du système et l'améliorer, une attention particulière étant accordée à la pseudonymisation, à la traçabilité et aux pratiques en matière de transfert de données.

35. Le CEPD souhaite que l'on insiste davantage sur la nécessité d'adopter de telles mesures dans le cadre de la directive proposée.

Renforcement des dispositions en matière de sécurité contenues dans la proposition

36. L'article 16 de la proposition, qui porte sur la protection des données à caractère personnel, la confidentialité et la sécurité de traitement, est libellé comme suit: «Les États membres veillent à ce que le droit fondamental de protection des données à caractère personnel soit pleinement et effectivement protégé dans toutes les activités de transplantation d'organes, conformément aux dispositions communautaires relatives à la protection des données à caractère personnel, et notamment l'article 8, paragraphe 3, l'article 16, l'article 17 et l'article 28, paragraphe 2, de la directive 95/46/CE». Le CEPD recommande d'ajouter un deuxième paragraphe, qui énoncera les principes fondamentaux permettant de garantir la sécurité au niveau des États membres, en incluant au moins les éléments suivants:

- mettre en place une politique de sécurité de l'information mettant en œuvre des mesures techniques et organisationnelles en vue d'assurer la confidentialité, l'intégrité, la responsabilité et la disponibilité à propos des données à caractère personnel des donneurs et des receveurs;
- définir et appliquer dans tous les États membres une politique spécifique en matière de confidentialité et de contrôle d'accès, l'objectif étant de préciser les droits d'accès, les rôles et les responsabilités des différentes parties concernées (donneur, organisme d'obtention, centre de transplantation, receveur, autorité nationale compétente, autorité compétente transfrontière) tout au long de la chaîne de traçabilité. Des garanties spécifiques en matière de confidentialité des données devraient être prévues à l'égard des personnes qui interviennent dans le traitement des données, en particulier si celles-ci ne sont pas liées par le secret médical (par exemple, codes de conduite en matière de confidentialité et mesures axées sur la responsabilité);
- préciser qu'il est nécessaire d'inclure des mécanismes de sécurité (tels que l'encryptage et les certificats numériques) dans les bases de données nationales. Pour ce qui concerne en particulier les registres des donneurs, il faudrait intégrer les principes de protection des données dès la phase de conception, afin de tenir compte de toutes les exigences requises en matière de sécurité dès les premières étapes de la mise en œuvre de ces développements technologiques;
- instaurer des procédures visant à garantir les droits des donneurs et des receveurs en matière de protection des données, en particulier les droits d'accès et de rectification, ainsi que le droit à l'information. Il faudrait en outre accorder une attention particulière aux cas où les donneurs souhaitent retirer leur consentement ou ne sont pas acceptés (après caractérisation du donneur et de l'organe) en tant que donneurs. Il conviendrait, pour ces types de cas, d'élaborer une procédure spécifique et de fixer un délai pour la conservation des données;

⁽¹⁾ L'équivalent électronique d'une carte d'identité qui authentifie l'émetteur d'une signature électronique (source: http://www.ffiec.gov/ffiecfbase/booklets/e_banking/ebanking_04_appx_b_glossary.html).

⁽²⁾ Une infrastructure à clefs publiques (ICP) est un ensemble de matériels, logiciels, personnes, politiques et procédures nécessaires pour créer, gérer, stocker, distribuer et révoquer les certificats numériques (source: <http://www.wikipedia.org>).

- prévoir dans la politique de sécurité de l'information des mesures visant à garantir l'intégrité et la disponibilité ininterrompue des données. Le rôle que joue l'analyse du risque dans le domaine de la sécurité des informations devrait être complété en prévoyant des hypothèses en matière de gestion des incidents et de continuité des activités;
- soumettre les politiques de sécurité de l'information à une surveillance et un réexamen réguliers, notamment en recourant à des audits indépendants.

37. Le CEPD recommande que les éléments susmentionnés soient intégrés à l'article 16 et soient ensuite plus amplement précisés dans le cadre de l'article 25 relatif aux mesures d'application, en particulier au paragraphe 1, points a), b) et c).

IV. GARANTIES CONCERNANT LES ÉCHANGES TRANSFRONTIÈRES D'ORGANES

Harmonisation des normes de sécurité entre les États membres

38. En pratique, l'échange transfrontière d'organes impliquera toujours le traitement de données à caractère personnel, étant donné que, même si ces informations sont codées, les organes demeureront identifiables (indirectement) par l'intermédiaire des autorités nationales compétentes.
39. Le CEPD a déjà exprimé son avis sur les besoins en matière de sécurité que présente la protection des données à caractère personnel dans le cadre des soins de santé transfrontaliers en Europe, en insistant notamment sur la nécessité d'harmoniser les politiques de sécurité de l'information entre les États membres, de manière à atteindre un niveau valable de protection des données ⁽¹⁾. Il recommande que cet élément soit également mentionné dans la proposition actuelle, plus précisément dans le considérant 17, qui fait référence à la disposition de la directive 95/46/CE relative à la sécurité du traitement.

Mise en place du système de traçabilité

40. Le mécanisme de traçabilité qui doit être mis en place constitue en l'espèce un paramètre important de la sécurité transfrontière des données. À cette fin, outre les mesures de sécurité appliquées au niveau de l'État membre, il convient d'accorder une attention particulière aux possibilités de pseudonymisation pouvant être utilisées pour identifier les donneurs et les receveurs (par exemple, type de codification, possibilité de double codification, etc.) et à la nécessité de continuer à assurer l'interopérabilité avec le système d'identification des tissus et des cellules.
41. Le CEPD recommande de faire spécifiquement référence à ce point à l'article 25 de la directive proposée, relatif aux mesures d'application, en modifiant le paragraphe 1, point b), comme suit: «les procédures permettant d'assurer la traçabilité complète des organes, dont les exigences en matière d'étiquetage, tout en garantissant la confidentialité des données relatives aux donneurs et aux receveurs tout au long de la procédure de traçabilité et en préservant l'interopérabilité avec le système d'identification des tissus et cellules.»

Échange d'organes avec des pays tiers

42. Les besoins en matière de sécurité sont plus importants encore lorsque des données sont échangées avec des pays tiers, dans lesquels un niveau approprié de protection des données ne peut être toujours garanti. Des règles spécifiques s'appliquant au transfert de données à caractère personnel vers des pays tiers sont prévues aux articles 25 et 26 de la directive 95/46/CE. Le CEPD est conscient du fait que les exigences en matière de protection des données ne devraient pas nuire à la rapidité et à l'efficacité du transfert d'organes, qui sont des caractéristiques essentielles du système de don d'organes et peuvent même souvent être une question de vie ou de mort. Il conviendrait dès lors d'explorer les possibilités d'autoriser les transferts, même en cas d'absence d'un niveau global adéquat de protection des données dans le pays tiers. Dans ce cadre, il conviendrait de tenir compte du fait que, en raison de la nature indirecte de l'identification des personnes au niveau transfrontière, ainsi que du fait que les autorités nationales compétentes se chargent de la surveillance générale du système, les risques encourus sont probablement moins élevés qu'au niveau national ⁽²⁾.
43. À cette fin, le CEPD estime qu'il convient que l'autorité compétente qui est chargée de délivrer l'autorisation de transfert consulte l'autorité nationale de protection des données afin d'élaborer, en tenant compte des dérogations éventuelles prévues à l'article 26 de la directive 95/46/CE, le cadre nécessaire pour que le transfert des données relatives aux organes en provenance ou à destination de pays tiers se déroule en toute sécurité, mais aussi de manière rapide et efficace. Il recommande de faire référence à ce point à l'article 21, relatif à l'échange d'organes avec les pays tiers, ou dans le considérant correspondant 15.

Mesures d'application

44. Avant de conclure, le CEPD invite le législateur à veiller, dans le cadre de l'article 25, à ce que toutes les parties concernées, y compris le CEPD et le groupe de l'article 29, soient consultées chaque fois que des mesures d'application ayant une incidence sur la protection et la sécurité des données sont envisagées.

V. CONCLUSIONS

45. Le CEPD a pris acte de l'initiative visant à garantir des normes de qualité et de sécurité élevées pour les organes humains destinés à la transplantation, qui peut être considérée comme s'inscrivant dans le cadre de l'approche globale de la CE tendant à fixer des normes communes dans le but de promouvoir la disponibilité transfrontière des services de soins de santé dans toute l'Europe.
46. La proposition prend déjà en compte les besoins en matière de protection des données en ce qui concerne tant les donneurs que les receveurs d'organes, en particulier via l'obligation de préserver le caractère confidentiel de leur identité. Le CEPD regrette toutefois que certaines de ces dispositions soient vagues, ambiguës ou d'ordre général, et il recommande dès lors d'y apporter plusieurs modifications afin d'en renforcer le volet «la protection des données».

⁽¹⁾ Avis du CEPD du 2 décembre 2008 sur la proposition de directive relative à l'application des droits des patients en matière de soins de santé transfrontaliers.

⁽²⁾ Voir l'avis n° 4/2007 du groupe de l'article 29, p. 18, en ce qui concerne les données pseudonymisées et codées.

47. Le CEPD relève tout d'abord la contradiction actuelle entre les concepts de traçabilité et d'anonymat utilisés dans la proposition. À ce sujet, il recommande d'apporter des modifications précises à la terminologie utilisée dans certaines parties de la proposition (à savoir au considérant 16, à l'article 10, paragraphe 2, et à l'article 17), afin d'éviter les ambiguïtés et d'indiquer de manière explicite que les données ne sont pas anonymes, mais qu'il conviendrait de procéder à leur traitement en respectant des règles strictes en matière de confidentialité et de sécurité.
48. Il recommande en outre d'insister davantage sur la nécessité d'adopter des mesures de sécurité strictes au niveau national, ce qui pourrait se faire en ajoutant à l'article 16 un deuxième paragraphe qui décrit les principes de base permettant de garantir la sécurité au niveau de l'État membre et en clarifiant ensuite cette exigence dans le cadre des mesures d'application définies à l'article 25, paragraphe 1. Les principes de sécurité proposés comprennent notamment:
- a) l'adoption d'une politique de sécurité de l'information visant à assurer la confidentialité, l'intégrité, la responsabilité et la disponibilité à propos des données à caractère personnel des donneurs et des receveurs;
 - b) la définition d'une politique spécifique en matière de confidentialité et de contrôle d'accès, ainsi que des garanties pour que les personnes qui interviennent dans le traitement assurent la confidentialité des données;
 - c) l'inclusion de mécanismes de sécurité dans les bases de données nationales, en intégrant les principes de protection des données dès la phase de conception;
 - d) l'établissement de procédures visant à garantir les droits des donneurs et des receveurs en matière de protection des données, en particulier les droits d'accès et de rectification et le droit à l'information, en accordant une attention particulière aux cas où les donneurs souhaitent retirer leur consentement ou ne sont pas acceptés en tant que donneurs;
 - e) l'adoption de mesures visant à garantir l'intégrité et la disponibilité ininterrompue des données;
 - f) l'organisation de contrôles réguliers et d'audits indépendants portant sur les politiques de sécurité en vigueur.
49. En ce qui concerne les échanges transfrontières d'organes, le CEPD recommande de mentionner au considérant 17 de la proposition la nécessité d'harmoniser les politiques de sécurité de l'information entre les États membres. En outre, une attention particulière devrait être accordée aux possibilités de pseudonymisation pouvant être utilisées pour identifier les donneurs et les receveurs et à la nécessité de continuer à assurer l'interopérabilité avec le système d'identification des tissus et cellules. Il recommande de faire spécifiquement référence à ce point à l'article 25, paragraphe 1, point b), de la proposition.
50. En ce qui concerne l'échange d'organes avec des pays tiers, le CEPD recommande qu'il soit indiqué, à l'article 21 ou dans le considérant 15 correspondant de la proposition, que l'autorité compétente consultera l'autorité nationale chargée de la protection des données afin d'élaborer le cadre nécessaire pour que le transfert des données relatives aux organes en provenance ou à destination de pays tiers se déroule en toute sécurité, mais aussi de manière rapide et efficace.
51. Enfin, le CEPD recommande que, chaque fois que des mesures d'application ayant une incidence sur la protection et la sécurité des données, toutes les parties concernées, y compris le CEPD et le groupe de l'article 29, soient consultées.

Fait à Bruxelles, le 5 mars 2009

Peter HUSTINX

Contrôleur européen de la protection des données