



**2093-01/05/FR
WP 114**

**Document de travail relatif à une interprétation commune des dispositions de
l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995**

Adopté le 25 novembre 2005

Le groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 14 de la directive 97/66/CE.

Le secrétariat est assuré par la Commission européenne, DG Justice, Liberté et Sécurité, Direction C «Justice civile, droits fondamentaux et citoyenneté, protection des données», B-1049 Bruxelles, Belgique, Bureau: LX46 1/143
Adresse Internet :

NOTE DE SYNTHÈSE

Le présent document de travail indique comment l'article 26, paragraphe 1, de la directive 95/46 doit être interprété et appliqué par les responsables du traitement désireux de procéder à des transferts de données vers des pays qui n'assurent pas un niveau de protection adéquat au sens de l'article 25 de ladite directive.

Le groupe de travail a rédigé le présent document parce qu'il craint que les dispositions de l'article 26, paragraphe 1, ne fassent dans la pratique l'objet d'interprétations divergentes qui empêcheraient leur application uniforme dans les différents États membres.

Des craintes semblables ont été formulées dans le rapport de 2003 de la Commission européenne sur la mise en œuvre de la directive 95/46. Ce rapport rappelait que ni une approche excessivement stricte des dispositions des articles 25 et 26, ni une approche extrêmement laxiste de ces dispositions (et plus particulièrement, de l'article 26, paragraphe 1) ne seraient conformes aux objectifs qu'elles visent, à savoir parvenir à un juste équilibre entre la protection des personnes dont les données doivent être transférées vers des pays n'assurant pas un niveau de protection adéquat et, notamment, «les impératifs du commerce international et la réalité des réseaux mondiaux de télécommunications.»

En précisant les dérogations à l'article 26, paragraphe 1, et notamment en développant le chapitre 5 du document de travail WP12 sur les transferts internationaux de données que le groupe a précédemment adopté en juillet 1998, le présent document a cherché à maintenir un juste équilibre entre les intérêts susmentionnés.

Dans la section 1 du présent document, le groupe de travail donne un aperçu de la manière dont ces dispositions s'articulent avec d'autres pour constituer ensemble l'économie générale de la directive sur les transferts internationaux de données. Il fournit ensuite des éléments d'interprétation et des recommandations s'appliquant à l'ensemble des dispositions de l'article 26, paragraphe 1. L'un des éléments essentiels de cette interprétation est la nécessité d'interpréter les dispositions de l'article 26, paragraphe 1, au sens strict, un autre élément étant que les dérogations concernent pour la plupart des cas dans lesquels les risques pour la personne en cause sont relativement faibles ou où d'autres intérêts peuvent être considérés comme primant le droit de la personne concernée au respect de la vie privée.

La section 1 développe cette interprétation et formule diverses recommandations visant à encourager les responsables du traitement à assurer «une protection adéquate» dans le plus grand nombre de situations possible.

Dans la section 2, le document fournit des indications complémentaires sur la manière dont chacune des dérogations de l'article 26, paragraphe 1, doit être interprétée. Cette section s'étend plus particulièrement sur les notions de «consentement» et d'«exécution d'un contrat», qui sont les dérogations sur lesquelles les responsables du traitement souhaitent s'appuyer le plus souvent dans la pratique.

Le groupe de travail estime que le présent document sera utile pour préciser la façon dont les responsables du traitement peuvent et, parfois, doivent faire usage des dérogations prévues à l'article 26, paragraphe 1, et le considère comme un élément fondamental de sa politique relative aux transferts de données vers des pays tiers. Il convient donc de le lire en

liaison avec d'autres travaux réalisés par le groupe dans ce domaine, notamment ceux portant sur les «règles d'entreprise contraignantes», les clauses contractuelles types et le niveau adéquat de protection dans les pays tiers, en ce compris la «sphère de sécurité» (Safe Harbor).

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL établi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995¹,

Vu l'article 29 et l'article 30, paragraphe 1, point c), et paragraphe 3, de ladite directive, vu son règlement intérieur, notamment les articles 12 et 14:

A ADOPTÉ LE PRÉSENT DOCUMENT DE TRAVAIL:

INTRODUCTION

L'objet du présent document de travail est de développer le chapitre 5 du document de travail WP12 «Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive», adopté par le groupe de travail le 24 juillet 1998² et portant sur l'interprétation de l'article 26, paragraphe 1, de la directive 95/46/CE.

Les dispositions de l'article 26, paragraphe 1, prévoient qu'un responsable du traitement peut, dans certaines conditions, transférer des données personnelles vers un pays tiers par dérogation au principe de «protection adéquate», consacré par l'article 25 de la directive.

À la lumière de l'expérience acquise depuis l'adoption de ce document, le groupe de travail constate l'existence d'interprétations divergentes des dispositions de l'article 26, paragraphe 1, qui pourraient empêcher leur application uniforme dans les différents États membres.

Cet état de fait et la nécessité d'une réaction appropriée ont également été constatés par la Commission dans les conclusions de son rapport sur la mise en œuvre de la directive relative à la protection des données³. Ce document souligne les divergences importantes constatées entre les législations des États membres en ce qui concerne la mise en œuvre des articles 25 et 26 de la directive, et le risque, à terme, de favoriser le «forum shopping» dans les différents États membres, selon que ces dispositions sont interprétées de manière plus ou moins large⁴. L'expérience de certaines autorités nationales de protection des données vient corroborer ce risque.

¹ J.O. L 281 du 23/11/1995, p. 31, disponible à l'adresse suivante:
http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

² Document de travail 12/2001 «Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données» du 24 juillet 1998.

³ Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE), 15 mai 2003, COM(2003) 265 final.

⁴ Page 21 du rapport: «Une attitude trop laxiste de la part de certains États membres, outre d'être en contradiction avec la directive, risque d'affaiblir le niveau de protection dans l'UE dans son ensemble parce qu'avec la libre circulation garantie par la directive, les flux de données pourraient se diriger vers les points de sortie "les moins contraignants"».

Le groupe de travail estime donc qu'il est nécessaire, eu égard aux missions qui lui sont confiées par l'article 30, paragraphe 1, point a), de la directive, et afin de répondre aux conclusions de la Commission dans le rapport précité, de préciser le champ d'application de ces dispositions et d'en fournir des éléments d'interprétation complémentaires.

1. ARTICULATION DES DIFFERENTES DISPOSITIONS DE LA DIRECTIVE 95/46 RELATIVES AUX TRANSFERTS INTERNATIONAUX DE DONNEES, DONT L'ARTICLE 26, PARAGRAPHE 1

1.1 PRESENTATION DES DISPOSITIONS DE LA DIRECTIVE RELATIVES AUX TRANSFERTS INTERNATIONAUX DE DONNEES VERS DES PAYS TIERS

Pour interpréter les dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE, il convient de garder présent à l'esprit le cadre général dans lequel elles s'inscrivent, afin d'assurer une interprétation cohérente des différentes dispositions de la directive relatives aux transferts internationaux de données.

La directive 95/46/CE du 24 octobre 1995 offre différentes bases juridiques pour le transfert de données personnelles vers des pays tiers, dont celles prévues par l'article 26, paragraphe 1:

1. Caractère adéquat dans le pays destinataire: en premier lieu, l'article 25, paragraphe 1, énonce le principe général selon lequel «le transfert vers un pays tiers de données à caractère personnel [...] ne peut avoir lieu que si [...] le pays tiers en question assure un niveau de protection adéquat». Le niveau de protection des données doit être apprécié au regard de toutes les circonstances entourant une opération ou un ensemble d'opérations de transfert de données et en attachant une importance particulière à plusieurs éléments pertinents pour le transfert et énumérés à l'article 25, paragraphe 2.

Aux termes de l'article 249 CE, la directive lie les États membres destinataires quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant aux moyens. À cet égard, la directive considérée impose aux États membres l'obligation de veiller à ce que les données à caractère personnel ne soient pas transférées vers un pays tiers s'il ne garantit pas un niveau de protection adéquat, et stipule que l'appréciation de ce niveau adéquat s'effectue au regard de toutes les circonstances. Elle ne précise toutefois pas si une quelconque autorité doit être chargée d'apprécier le caractère adéquat de la protection des données dans les pays tiers. Il est donc possible que la législation nationale des États membres confie cette tâche à des instances nationales de protection des données, dont l'autorisation peut être requise pour procéder au transfert de données à caractère personnel vers un pays tiers.

Outre cette possibilité, prévue par la législation nationale, d'évaluation du caractère adéquat de la protection par des instances nationales, la directive dispose que des décisions sur le niveau de protection adéquat sont adoptées, à l'échelle européenne, par la Commission, apportant ainsi une valeur ajoutée en termes de sécurité juridique et d'uniformité dans l'ensemble de la Communauté. En vertu de l'article 25, paragraphe 6, la Commission peut reconnaître que

certaines pays assurent un niveau de protection adéquat, auquel cas les transferts de données à caractère personnel peuvent s'effectuer vers ces pays sans devoir remplir d'exigence formelle spécifique. C'est le cas désormais des transferts internationaux de données vers des destinataires établis en Suisse, au Canada, en Argentine, à Guernesey ou sur l'Île de Man, ou dont le destinataire est une entreprise américaine ayant adhéré à la «sphère de sécurité» (Safe Harbor)⁵. Le transfert au Bureau américain des douanes et de la protection des frontières des dossiers passagers relatifs aux vols en provenance et à destination des États-Unis, en application d'une décision de la Commission envers laquelle le présent groupe de travail s'est montré très critique, s'est également fondé sur cette base juridique.

2. Garanties suffisantes mises en place par le destinataire: en deuxième lieu, un État membre peut également, en vertu de l'article 26, paragraphe 2, de la directive, autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat lorsque le responsable du traitement offre des «garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants.»

L'article 26, paragraphe 2, in fine, indique en outre que ces garanties «peuvent notamment résulter de clauses contractuelles appropriées». Afin de faciliter le recours à cette solution contractuelle, la Commission européenne a émis trois décisions relatives à des clauses contractuelles types, dont deux réglementent les transferts de responsable du traitement à responsable du traitement, et la troisième les transferts de responsable du traitement à sous-traitant⁶.

Par ailleurs, outre la possibilité de recourir à des clauses contractuelles pour mettre en place ces garanties suffisantes, le groupe «article 29» travaille activement, depuis l'année 2003, sur la possibilité pour les groupes multinationaux, d'utiliser aux mêmes fins des «règles d'entreprise contraignantes»⁷.

3. Déroptions prévues par l'article 26, paragraphe 1: en troisième lieu, l'article 26, paragraphe 1, de la directive prévoit que des transferts de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat peuvent être effectués si l'une des conditions suivantes est remplie:
 - a) la personne concernée a indubitablement donné son consentement au transfert envisagé;

⁵ Les informations relatives à ces pays et au dispositif de la «sphère de sécurité» (Safe Harbor) sont disponibles à l'adresse suivante: http://europa.eu.int/comm/internal_market/privacy/adequacy_fr.htm

⁶ En ce qui concerne les transferts de responsable du traitement à responsable du traitement, la Commission a émis une première série de clauses contractuelles types le 15 juin 2001; elle a ensuite amendé cette décision aux fins d'y annexer un nouvel ensemble de clauses alternatives aux premières (décision du 27 décembre 2004). En ce qui concerne les transferts de responsable du traitement à sous-traitant, la Commission a émis une série de clauses contractuelles types le 27 décembre 2001. Les textes de toutes ces clauses sont disponibles à l'adresse suivante: http://europa.eu.int/comm.internal_market/privacy/modelcontracts_fr.htm

⁷ Cf. le document de travail WP 74, «Transferts de données personnelles vers des pays tiers: Application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données», adopté par le groupe le 3 juin 2003 et les documents complémentaires WP107 et WP108.

- b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée;
- c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers;
- d) le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice;
- e) le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée;
- f) le transfert intervient au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

Dans les cas énoncés dans les sections 1 et 2 ci-dessus, le transfert a lieu dans des conditions faisant en sorte que les personnes concernées continuent à bénéficier d'une protection au regard du traitement de leurs données, une fois celles-ci transférées. Cette protection est assurée soit par la législation générale ou la réglementation sectorielle en vigueur dans le pays où le destinataire est établi, soit par les garanties suffisantes fournies par le responsable du traitement dans la Communauté, en particulier compte tenu d'engagements contraignants souscrits par le destinataire quant au traitement des données transférées vers ce pays tiers.

À l'inverse, l'article 26, paragraphe 1, prévoit de véritables dérogations au principe de protection adéquate institué par l'article 25 de la directive. En fait, ces dérogations permettent le transfert vers des pays tiers qui n'assurent pas un niveau de protection adéquat. À plus forte raison, elles pourraient également servir de base juridique lorsque le pays tiers assure bel et bien un niveau de protection adéquat mais que ce caractère adéquat n'a pas fait l'objet d'une évaluation. Même si le recours aux dérogations n'implique pas en soi, dans tous les cas, que le pays de destination n'assure pas un niveau de protection adéquat, il n'est pas la garantie du contraire non plus. En conséquence, la personne dont les données ont été transférées, même avec son consentement, pourrait se trouver totalement dénuée de protection dans le pays destinataire, du moins au sens des dispositions de l'article 25 ou de l'article 26, paragraphe 2, de la directive 95/46.

Compte tenu de cette différence importante en termes de protection, il est essentiel que ces différentes bases juridiques soient utilisées de manière cohérente, compte tenu du système global dans lequel elles s'inscrivent.

1.2 LA POSITION DE L'ARTICLE 26, PARAGRAPHE 1, DANS L'ECONOMIE DE LA DIRECTIVE

La juxtaposition de ces différentes règles relatives aux transferts de données personnelles peut donner une impression paradoxale et être aisément source de malentendus.

D'une part, une première série de dispositions - celles de l'article 25, paragraphe 1, de l'article 25, paragraphe 6, et de l'article 26, paragraphe 2 - visent à garantir que les

données à caractère personnel qui sont transférées continuent à bénéficier d'une protection adéquate après leur transfert vers le pays de destination. Ces transferts peuvent avoir lieu soit parce que le cadre juridique du pays tiers concerné assure une protection adéquate, soit parce que cette protection est garantie par des clauses contractuelles types ou d'autres garanties appropriées, comme la conclusion d'un contrat, l'adoption de règles d'entreprise contraignantes ou l'autocertification en vue de se conformer aux principes de la «sphère de sécurité» (Safe Harbor), etc. De surcroît, comme indiqué plus haut, plusieurs législations nationales disposent que certains transferts peuvent également être soumis à une autorisation ou à l'avis préalable des instances nationales compétentes (dans la plupart des cas, les instances de protection des données).

D'autre part, une seconde série de dispositions, à savoir celles de l'article 26, paragraphe 1, facilitent grandement le transfert de données personnelles vers un pays tiers. Aux termes de celles-ci, le responsable du traitement à l'origine du transfert n'a ni à s'assurer de l'existence d'une protection adéquate chez le destinataire ni à obtenir, normalement, une quelconque autorisation préalable du transfert par les autorités compétentes, au cas où cette procédure serait applicable. Elles n'obligent pas davantage le destinataire des données à se conformer aux dispositions de la directive quant au traitement des données dans son propre pays (par exemple, principes de finalité, sécurité, droit d'accès, etc.).

Si l'on s'en tenait à la lettre de la directive, on pourrait conclure à une incohérence majeure de ses dispositions relatives aux transferts de données à caractère personnel vers des pays tiers. Après tout, la logique qui sous-tend le principe de protection adéquate consacré par l'article 25 est de garantir aux personnes qu'elles continuent à bénéficier des droits et libertés fondamentaux qui leur sont octroyés à l'égard du traitement de leurs données dans l'Union européenne, une fois que celles-ci ont été transférées vers un pays tiers. Elle vise également à éviter le contournement de la protection accordée par les législations européennes de protection des données à caractère personnel par le transfert des données vers des pays tiers.

Cette dualité apparente des principes s'explique notamment par la reconnaissance du fait que l'expansion du commerce international rend nécessaire, dans certains cas, la flexibilité des transferts internationaux de données, y compris des transferts d'informations à caractère personnel (comme l'expose le considérant 56 de la directive).

Cette incohérence apparente peut toutefois également s'expliquer par le fait que l'article 26, paragraphe 1, a été conçu pour régler un nombre limité de cas dans lesquels une dérogation à l'exigence de «protection adéquate» pour les transferts vers les pays tiers a été considérée appropriée. Comme le groupe de travail l'indiquait déjà dans le document WP12: «Ces dérogations, formulées de manière restrictive, concernent, pour l'essentiel, des cas où les risques pour la personne concernée sont relativement faibles ou des situations dans lesquelles d'autres intérêts (qu'ils soient publics ou propres à la personne concernée elle-même) priment le droit de la personne concernée au respect de la vie privée. Ces exceptions qui constituent des dérogations à un principe général doivent de ce fait être interprétées de manière restrictive. Les États membres peuvent en outre prévoir dans leur droit national que ces dérogations ne s'appliquent pas dans certains cas, par exemple lorsqu'il est nécessaire de protéger des catégories particulièrement vulnérables, telles que les travailleurs ou les malades.»

Dans la pratique, les responsables du traitement ont toutefois eu tendance à faire un usage préférentiel de ces dérogations, même s'il était inopportun.

En conséquence, le groupe de travail voudrait avant tout faire en sorte que la signification et la portée de l'article 26, paragraphe 1, soient bien comprises par toutes les personnes concernées, afin d'éviter que les responsables du traitement n'utilisent les dérogations à mauvais escient. Cela requiert une interprétation claire et commune de l'article 26, paragraphe 1, proprement dit, et de sa position dans l'économie générale de la directive.

Cet exercice doit être régi par le principe que, comme le groupe l'a indiqué précédemment dans son document de travail WP12 précité, l'interprétation de l'article 26, paragraphe 1, doit nécessairement être stricte.

À cet égard, le groupe de travail souligne que cette logique correspond à celle du Protocole additionnel à la Convention 108. Le rapport explicatif de ce texte prévoit en effet que «les Parties possèdent une marge d'appréciation pour déterminer les dérogations au principe de niveau adéquat. Les règles pertinentes de droit interne doivent néanmoins respecter le principe de droit inhérent à l'ordre juridique européen qui consiste à interpréter les clauses d'exception de manière restrictive afin que l'exception ne devienne pas la règle⁸».

De manière plus générale, cette règle d'interprétation stricte découle aussi clairement de la jurisprudence de la Cour européenne des droits de l'homme, qui interprète les droits fondamentaux de façon assez large, conformément au principe dit «*d'effet utile*» de la protection accordée, afin de limiter la portée des dérogations à ce principe. La Cour a appliqué ce principe dans plusieurs affaires importantes⁹.

Le groupe de travail confirme donc explicitement son interprétation de l'article 26, paragraphe 1, telle que précédemment exposée, et l'explique dans la section 2 du présent document de travail.

Cependant, il convient aussi de noter que les dispositions de la directive relatives aux transferts de données à caractère personnel vers des pays tiers ne peuvent être appliquées séparément des autres dispositions de la directive. Comme le stipule explicitement l'article 25, paragraphe 1, ces dispositions s'appliquent «sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive». Cela signifie que quelles que soient les dispositions sur lesquelles on se fonde pour le transfert de données vers un pays tiers, il y a lieu de respecter les autres dispositions pertinentes de la directive.

Cela signifie plus particulièrement, conformément au soixantième considérant du préambule de la directive, que si des données sensibles sont concernées par le transfert, il convient de respecter les dispositions de l'article 8 de la directive. Cela peut avoir pour conséquence qu'un transfert particulier ne peut se fonder sur l'article 26, paragraphe 1, le cas échéant, que si les conditions de l'article 8 sont remplies. En d'autres termes, même si la législation nationale n'a pas fait usage de la possibilité de limiter la portée de

⁸ Cf. rapport explicatif sur le Protocole additionnel à la Convention 108 concernant les autorités de contrôle et les flux transfrontières de données, article 2, paragraphe 2, point a); ce document est accessible à l'adresse suivante: <http://conventions.coe.int/Treaty/FR/Reports/Html/181.htm>

⁹ Affaires Delcourt (17 janvier 1970) et Klass (6 septembre 1978)

l'article 26, paragraphe 1, pour certaines catégories de cas, des restrictions supplémentaires pourraient résulter d'autres dispositions de la directive.

Le groupe de travail tient également à mentionner que les principes de «traitement loyal et licite» et d'«utilisation compatible» énoncés à l'article 6, paragraphe 1, points a) et b), continuent à s'appliquer à cet égard. Cela peut signifier que le responsable du traitement ait l'obligation de communiquer aux personnes concernées des informations pertinentes sur les transferts de données vers un pays tiers, même si les articles 10, 11 ou 26, paragraphe 1, ne l'exigent pas. De même, il peut arriver qu'une personne concernée ait une raison de s'opposer à des transferts particuliers «pour des raisons prépondérantes et légitimes tenant à sa situation particulière», comme le prévoit l'article 14, point a), de la directive. Cette objection peut également porter sur des données personnelles qui ne sont pas sensibles au sens de l'article 8 de la directive ou au sens de ce que la personne concernée pourrait considérer comme des données sensibles la concernant dans une situation particulière (par exemple, données financières, données permettant l'adaptation d'une décision négative à l'encontre de la personne concernée en termes de gestion de l'entreprise, etc.).

1.3 RECOMMANDATIONS SUR L'UTILISATION RESPECTIVE DES DIFFERENTES BASES JURIDIQUES OFFERTES PAR LA DIRECTIVE POUR LES TRANSFERTS INTERNATIONAUX DE DONNEES

Sans préjudice de l'interprétation générale de l'article 26, paragraphe 1, au point 1.2 du présent document de travail, ni de l'interprétation particulière de chaque dérogation dans la section 2 ci-après, le groupe de travail souhaite par ailleurs formuler plusieurs recommandations quant à l'utilisation respective des différentes bases juridiques offertes par la directive pour les transferts de données vers des pays tiers.

Ces recommandations sont formulées au chapitre 5 du document WP12. Elles visent à encourager les responsables du traitement à assurer une «protection adéquate» dans le plus grand nombre de situations possible. Le groupe de travail a déjà déclaré que, lorsqu'ils envisagent de procéder à un transfert de données vers un pays tiers, les responsables du traitement établis dans l'Union européenne doivent privilégier des solutions garantissant aux personnes qu'elles continueront à bénéficier des droits et garanties fondamentaux reconnus à l'égard du traitement de leurs données dans l'UE, une fois celles-ci transférées.

Par conséquent, une approche fondée sur les meilleures pratiques consisterait, pour un responsable du traitement envisageant un transfert international de données, à examiner d'abord si le pays tiers garantit un niveau de protection adéquat et à s'assurer que les données exportées y seront sauvegardées. En cas d'exportations vers les États-Unis, l'exportateur responsable pourrait souhaiter encourager l'importateur à souscrire aux principes de la «sphère de sécurité» (Safe Harbor). Si le niveau de protection dans le pays tiers n'est pas adéquat eu égard à toutes les circonstances entourant un transfert de données, le responsable du traitement des données devrait envisager le recours à l'article 26, paragraphe 2, c'est-à-dire d'obtenir des garanties adéquates au moyen, par exemple, de clauses contractuelles types ou de règles d'entreprise contraignantes. Ce n'est que si cela n'est vraiment pas pratique et/ou faisable qu'il devrait envisager d'utiliser les dérogations de l'article 26, paragraphe 1.

Dans le droit fil de cette logique, le groupe de travail recommande que les dérogations de l'article 26, paragraphe 1, de la directive s'appliquent de préférence aux cas dans lesquels il serait vraiment inapproprié voire impossible que le transfert s'effectue sur la base de l'article 26, paragraphe 2.

Le groupe de travail trouverait regrettable qu'une société multinationale ou une autorité publique envisage d'effectuer des transferts importants de données vers un pays tiers sans prévoir un cadre approprié à cet effet, alors qu'elle a les moyens pratiques d'assurer cette protection (par exemple, un contrat, une règle d'entreprise contraignante, une convention).

C'est notamment pour cette raison que le groupe de travail recommande que les transferts de données personnelles qui pourraient être qualifiés de répétés, massifs ou structurels soient, dans toute la mesure du possible et justement en raison de ces caractéristiques, effectués dans un cadre juridique spécifique (c'est-à-dire des contrats ou des règles d'entreprise contraignantes). Le groupe de travail reconnaît par ailleurs que, dans certains cas, des transferts massifs ou répétés peuvent être légitimement effectués sur la base de l'article 26, paragraphe 1, lorsque le recours au cadre juridique susmentionné est impossible dans la pratique, que les risques pour la personne concernée sont faibles et que les articles 6, 7 et 8 sont appliqués correctement. On peut citer comme exemple pertinent celui de transferts internationaux de fonds qui ont encore lieu quotidiennement et massivement.

Le groupe de travail recommande donc, même dans certaines situations où la légitimité du transfert résulterait de l'un des cas énoncés à l'article 26, paragraphe 1, que des éléments supplémentaires tels que l'ampleur du transfert envisagé ou les risques induits pour les personnes concernées amènent le responsable du traitement à conclure un contrat ou à élaborer des règles d'entreprises contraignantes en vue de l'effectuer.

Enfin, il va de soi que le recours aux dérogations de l'article 26, paragraphe 1, ne doit jamais conduire à une situation dans laquelle il pourrait y avoir violation des droits fondamentaux.

Lorsqu'il a introduit ces dérogations au principe de protection adéquate dans la directive, le législateur européen a considéré qu'elles étaient justifiées pour autant qu'elles soient jugées compatibles avec la protection des droits fondamentaux des personnes et avec la libre circulation de l'information au niveau international. En d'autres termes, si les cas énumérés à l'article 26, paragraphe 1, peuvent constituer une dérogation au principe voulant que le pays tiers garantisse une protection adéquate, ils ne constituent pas des dérogations supplémentaires à la règle prescrivant le respect des droits fondamentaux.

Les instances nationales de protection des données doivent faire en sorte que ces dérogations soient appliquées dans des situations qui n'entraînent pas une violation des droits fondamentaux des personnes concernées et qui correspondent au besoin de maintenir une stricte interprétation de ces dérogations. À cet égard, elles peuvent, s'il y a des raisons suffisantes de le faire, intervenir à tout moment et recommander qu'un transfert international de données s'effectue sur la base de garanties adéquates au sens de l'article 26, paragraphe 2, plutôt qu'en application des dérogations énumérées à l'article 26, paragraphe 1.

2. INTERPRETATION PARTICULIERE DES DISPOSITIONS DE L'ARTICLE 26, PARAGRAPHE 1

Outre les observations générales formulées dans la section précédente, le groupe de travail souhaite également donner certaines indications sur le sens précis de chacune des dérogations prévues par l'article 26, paragraphe 1. Ces indications ont été rédigées compte tenu de l'expérience acquise en la matière par le groupe et par les autorités nationales de protection des données personnelles et étant entendu que la formulation des dérogations doit se comprendre dans son acception naturelle, c'est-à-dire qu'elle ne doit être ni artificiellement restreinte ni artificiellement étendue.

2.1 CONSENTEMENT (ARTICLE 26, PARAGRAPHE 1, POINT A))

L'article 26, paragraphe 1, point a), prévoit qu'un transfert de données à caractère personnel peut être effectué vers un pays n'assurant pas un niveau de protection adéquat à condition que «la personne concernée ait indubitablement donné son consentement au transfert envisagé».

Comme le groupe de travail l'a déjà indiqué dans son précédent document de travail WP 12, il importe de garder à l'esprit que pour être valable, ce consentement doit, quelles que soient les circonstances dans lesquelles il est donné, être une manifestation de volonté, libre, spécifique et informée, selon la définition qu'en donne l'article 2, point h), de la directive.

- Le consentement doit être une manifestation de volonté claire et indubitable

L'importance du fait que le consentement soit un acte positif exclut de facto tout système par lequel la personne concernée n'aurait le droit de s'opposer au transfert *qu'après* qu'il a eu lieu: le consentement spécifique à un transfert doit être authentiquement exigé pour que celui-ci puisse avoir lieu. Tout doute au sujet de la réalité du consentement rendrait la dérogation inapplicable. Donc, comme l'indique le groupe de travail dans son document WP12, «cela signifiera vraisemblablement que de nombreuses situations où le consentement est implicite (par exemple, parce qu'une personne a eu connaissance d'un transfert, sans s'y opposer) ne pourront pas être couvertes par cette dérogation».

Par ailleurs, dans son avis relatif à l'interprétation de l'article 13 de la directive «vie privée et communications électroniques»¹⁰, qui a introduit un régime harmonisé pour les communications à des fins de prospection directe aux personnes physiques, le groupe de travail a fourni des éléments d'interprétation de la notion de «consentement préalable» dans le contexte spécifique des communications électroniques et dans celui d'Internet, en particulier. Il est utile de renvoyer à ces indications dans le présent document, puisque le consentement de la personne concernée à un transfert peut parfois être demandé en ligne. Le groupe de travail a particulièrement recommandé l'utilisation sur les sites Internet de cases à cocher, afin de recueillir le consentement préalable de la personne; l'utilisation de cases pré-cochées ne remplit pas la condition voulant que le consentement soit une manifestation de volonté claire et indubitable.

- Le consentement doit être donné librement

¹⁰ Avis 5/2004 portant sur les communications de prospection directe non sollicitées selon l'article 13 de la directive 2002/58/CE, WP 90, du 27 février 2004, point 3.2.

Un consentement donné par une personne concernée qui n'a pas eu la possibilité d'effectuer un véritable choix ou qui a été mise devant le fait accompli ne peut être considéré comme valable.

C'est pourquoi le groupe de travail a examiné si le consentement peut être valablement utilisé pour le transfert aux autorités américaines des données de réservation («données PNR») des compagnies aériennes européennes. On pouvait en effet se demander si le consentement des passagers aurait pu être librement donné puisque les compagnies aériennes sont obligées d'envoyer les données avant le départ du vol, et que les passagers n'ont donc pas de véritable choix s'ils souhaitent voyager¹¹.

À cet égard, le groupe de travail tient à attirer l'attention sur les difficultés particulières qui pourraient surgir pour considérer le consentement d'une personne concernée comme donné librement dans une relation d'emploi, en raison du lien de subordination entre l'employeur et le salarié¹². Dans ce contexte, un consentement valable signifie que le salarié doit avoir une possibilité réelle de refuser son consentement sans subir un préjudice ou de le retirer ultérieurement s'il change d'avis. Dans de telles situations de dépendance hiérarchique, le refus ou les réserves d'un salarié à l'égard d'un transfert pourraient en effet lui causer un préjudice moral ou matériel, ce qui est tout à fait contraire à la lettre et à l'esprit de la législation européenne en matière de protection des données personnelles. Le groupe de travail reconnaît toutefois l'existence de cas où il est opportun que l'employeur s'appuie sur un consentement, par exemple dans une organisation internationale où les salariés souhaitent tirer profit de possibilités offertes dans un pays tiers.

En conséquence, le groupe de travail invite les employeurs à ne pas se fonder uniquement sur le consentement de leurs salariés pour le transfert de leurs données, sauf dans les cas où il est avéré que les salariés ne subiraient aucune conséquence s'ils ne souhaitaient pas donner leur consentement à un transfert ou si, après l'avoir donné, ils souhaitaient le retirer, dans le cas où ce serait possible.

De surcroît, à la lumière de l'expérience acquise, le groupe de travail estime que le consentement n'est pas susceptible de fournir un cadre adéquat à long terme pour les responsables du traitement, en cas de transferts répétitifs ou même structurels pour le traitement en question. De fait, et en particulier si le transfert fait partie intrinsèque du traitement principal (par exemple, la centralisation d'une base de données mondiale de ressources humaines, dont le fonctionnement nécessite des transferts de données permanents et systématiques), les responsables du traitement risqueraient de se trouver eux-mêmes dans des situations insolubles si ne fût-ce qu'une personne concernée par le transfert décidait ultérieurement de retirer son consentement. Les données concernant une personne ayant retiré son consentement ne pourraient plus stricto sensu faire l'objet d'un transfert; à défaut, le transfert resterait partiellement fondé sur le consentement de personnes concernées, mais une solution de remplacement (contrat, règles d'entreprises contraignantes, etc.) devrait être trouvée pour les données des personnes ayant retiré leur consentement. Le recours au consentement peut donc se révéler être une «fausse bonne solution», simple de prime abord, mais en réalité complexe et lourde à gérer.

¹¹ Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis.

¹² Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel et note de synthèse correspondante, en date du 13 septembre 2001.

- Le consentement doit être spécifique

Pour constituer une base juridique valable pour un éventuel transfert de données, le consentement de la personne concernée doit en outre être spécifiquement donné pour le transfert ou la catégorie de transferts dont il s'agit.

Le consentement devant être spécifique, il est parfois impossible d'obtenir celui de la personne concernée préalablement à un futur transfert, notamment si la survenance et les circonstances précises du transfert ne sont pas connues au moment où le consentement est demandé et que l'incidence sur la personne concernée ne peut donc être appréciée. À titre d'exemple, une entreprise ne pourra pas, au moment où elle collectera les données de ses clients dans un but précis, leur demander de consentir par anticipation au transfert de leurs données vers un pays tiers, dans l'éventualité où cette entreprise se ferait racheter par une entreprise tierce. Toutefois, il est envisageable qu'une personne puisse valablement consentir par anticipation au transfert de ses données vers un pays tiers lorsque les détails de ce transfert sont déjà prédéterminés, notamment en termes de finalité et de catégories de destinataires.

- Le consentement doit être informé

Cette condition revêt une importance particulière. Elle impose que la personne concernée ait été correctement informée à l'avance des circonstances particulières du transfert (finalité du transfert, identité et coordonnées du ou des destinataires, etc.), conformément au principe général de loyauté.

Les informations données aux personnes concernées doivent également comprendre le risque spécifique résultant du fait que les données les concernant seront transférées vers un pays n'assurant pas une protection adéquate. Seule cette information leur permettra de donner leur consentement en pleine connaissance de cause; si elle n'est pas fournie, la dérogation ne s'appliquera pas.

Le groupe de travail a constaté que le consentement était parfois compliqué à obtenir en raison de problèmes pratiques, notamment en l'absence de contact direct entre le responsable du traitement et les personnes concernées (même si la solution prévue par l'article 26, paragraphe 2, s'avère parfois plus aisée à mettre en œuvre). Quelles que puissent être ces difficultés, le responsable du traitement doit pouvoir prouver en toutes circonstances, d'une part, qu'il a obtenu le consentement de chaque personne concernée et, d'autre part, que ce consentement a été donné sur la base d'informations suffisamment précises, y compris quant à l'absence de protection dans le pays tiers.

2.2 TRANSFERT NECESSAIRE A L'EXECUTION D'UN CONTRAT ENTRE LA PERSONNE CONCERNEE ET LE RESPONSABLE DU TRAITEMENT OU A L'EXECUTION DE MESURES PRECONTRACTUELLES PRISES A LA DEMANDE DE LA PERSONNE CONCERNEE (ARTICLE 26, PARAGRAPHE 1, POINT b))

Dans son document de travail WP12, le groupe de travail a précisé que, bien que la portée de ces dérogations relatives à l'exécution du contrat semble potentiellement très vaste, leur application sera, dans la pratique, limitée par le critère de «nécessité».

Le groupe de travail est en effet conscient du fait que, indépendamment de l'interprétation générale de l'article 26, paragraphe 1, et des nouvelles recommandations formulées dans la section 1.3. du présent document, ce «critère de nécessité» pourrait limiter en soi le nombre de cas où il peut être recouru aux différentes dérogations de l'article 26, paragraphe 1, qui se réfèrent à cette notion de «nécessité» (article 26, paragraphe 1, points b) à e)).

Dans le cas de l'article 26, paragraphe 1, point b), un transfert de données vers un pays tiers n'assurant pas un niveau de protection adéquat ne peut être réputé relever de la dérogation de l'article 26, paragraphe 1, point b), que s'il peut être considéré comme *nécessaire* à l'exécution du contrat en question ou de mesures précontractuelles prises à la demande de la personne concernée. Ce «critère de nécessité» exige dans ce cas un lien étroit et important entre la personne concernée et la finalité du contrat.

Ainsi, certains groupes internationaux souhaiteraient pouvoir recourir à cette dérogation pour transférer des données relatives à leurs salariés d'une filiale vers la société mère, afin, par exemple, de centraliser les activités de gestion des salaires et des ressources humaines de l'ensemble du groupe. Elles estiment que ces transferts pourraient être considérés comme nécessaires à l'exécution du contrat de travail conclu entre le salarié et le responsable du traitement. Le groupe de travail juge cette interprétation excessive, car il est très douteux que la notion de contrat de travail puisse être interprétée aussi largement, puisqu'il n'y a pas de lien direct et objectif entre l'exécution d'un contrat de travail et un tel transfert de données.

De surcroît, une interprétation stricte de cette dérogation implique que les données transférées doivent être réellement nécessaires à la finalité de l'exécution de ce contrat ou de ces mesures précontractuelles.

C'est pourquoi, dans son avis du 24 octobre 2002 sur les données passagers, le groupe de travail a refusé de considérer que cette condition pouvait s'appliquer aux transferts de données relatives aux passagers des compagnies aériennes aux autorités américaines, en raison de la nature des données transmises, dont certaines ne peuvent être considérées comme «nécessaires» à l'exécution du contrat de transport¹³.

À l'inverse, cette dérogation constituerait une base juridique acceptable pour le transfert par des agences de voyage de données personnelles relatives à leurs clients à des hôtels ou d'autres partenaires commerciaux qui interviendraient dans l'organisation du séjour de ces clients.

Enfin, cette dérogation ne peut s'appliquer aux transferts de données supplémentaires non essentielles à la finalité du transfert ou aux transferts dans un but autre que l'exécution du contrat. Plus généralement, les dérogations de l'article 26, paragraphe 1, points b) à e), ne permettent que le transfert des données nécessaires à la finalité du transfert; pour les autres données, il convient de trouver d'autres moyens de prouver le caractère adéquat du transfert.

¹³ Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis.

2.3 TRANSFERT NECESSAIRE A LA CONCLUSION OU A L'EXECUTION D'UN CONTRAT CONCLU OU A CONCLURE, DANS L'INTERET DE LA PERSONNE CONCERNEE, ENTRE LE RESPONSABLE DU TRAITEMENT ET UN TIERS (ARTICLE 26, PARAGRAPHE 1, POINT c))

Cette disposition a nécessairement la même interprétation que la précédente, à savoir qu'un transfert de données vers un pays tiers n'assurant pas un niveau de protection adéquat ne peut être réputé relever de la dérogation de l'article 26, paragraphe 1, point c), que s'il peut être considéré comme réellement «nécessaire à la conclusion ou à l'exécution d'un contrat entre le responsable du traitement et un tiers, dans l'intérêt de la personne concernée» et qu'il satisfait au «critère de nécessité» correspondant. Dans le cas présent, ce critère exige un lien étroit et important entre l'intérêt de la personne concernée et la finalité du contrat.

Certains responsables du traitement ont parfois exprimé le souhait de recourir à cette dérogation comme base des transferts internationaux de données concernant leurs salariés à des prestataires de services établis en dehors de l'UE, auprès desquels ils externalisent leur gestion des salaires. Ces transferts seraient, selon eux, nécessaires à l'exécution de leur contrat de sous-traitance et seraient dans l'intérêt des personnes concernées, puisque leur finalité est la gestion des salaires du personnel. Dans ce cas de figure, le groupe de travail estime toutefois que le lien étroit et important entre l'intérêt des personnes concernées et la finalité du contrat n'est pas établi et que la dérogation ne peut s'appliquer.

De même, certains groupes internationaux souhaiteraient pouvoir faire usage de cette dérogation pour la gestion de programmes de «stock options» dont ils font bénéficier certaines catégories de leur personnel. À cet effet, ils ont normalement recours à des prestataires financiers spécialisés dans la gestion de tels programmes, établis dans des pays tiers. Ces groupes estiment que les transferts pourraient ainsi avoir lieu vers ce prestataire aux fins de l'exécution du contrat conclu entre lui et le responsable du traitement, dans l'intérêt des bénéficiaires du programme.

Comme le groupe de travail a des réserves au sujet de la validité de cette interprétation, le responsable du traitement qui souhaiterait fonder ces arrangements sur l'article 26, paragraphe 1, point c), devrait démontrer à la satisfaction d'une instance de protection des données que les données transférées sont nécessaires à l'exécution de ce contrat, conformément à l'interprétation stricte du terme «nécessaire» mentionnée plus haut.

Le groupe de travail tient à préciser que cette interprétation ne signifie en aucun cas qu'il porte un jugement négatif sur le choix, par les responsables du traitement, de gestionnaires de données établis dans des pays tiers. Il entend simplement insister sur l'opportunité de se fonder sur un instrument prévu par l'article 26, paragraphe 2 (dans la pratique, un contrat), pour procéder à des transferts de données en pareils cas.

2.4 TRANSFERT NECESSAIRE OU RENDU JURIDIQUEMENT OBLIGATOIRE POUR LA SAUVEGARDE D'UN INTERET PUBLIC IMPORTANT, OU POUR LA CONSTATATION, L'EXERCICE OU LA DEFENSE D'UN DROIT EN JUSTICE (ARTICLE 26, PARAGRAPHE 1, POINT d))

Les dérogations prévues par l'article 26, paragraphe 1, point d), doivent obéir à une même règle d'interprétation stricte que celle appliquée dans les paragraphes précédents.

Le groupe de travail a déjà donné une interprétation restrictive de la notion de «sauvegarde d'un intérêt public important» dans son avis sur les données passagers du 24 octobre 2002¹⁴. Il s'est opposé au recours à cette dérogation pour justifier le transfert de données relatives aux passagers des compagnies aériennes aux autorités américaines au titre de la sauvegarde d'un intérêt public important pour deux raisons: d'une part, la nécessité du transfert n'avait pas été établie et, d'autre part, il ne paraissait pas acceptable qu'une décision unilatérale d'un pays tiers, pour des raisons d'intérêt public qui lui sont propres, conduise à des transferts réguliers et massifs de données protégées par la directive.

À cet égard, il est évident que les rédacteurs de la directive ont envisagé que seuls des intérêts publics importants, définis comme tels par la loi nationale applicable aux responsables du traitement établis dans l'UE, puissent être valablement pris en compte dans ce contexte. Toute autre interprétation permettrait à une autorité étrangère de contourner aisément l'exigence d'un niveau de protection adéquat dans le pays destinataire que prévoit la directive 95/46.

D'autre part, le considérant 58 de la directive 95/46 mentionne, en ce qui concerne cette disposition, les cas dans lesquels des échanges internationaux de données pourraient être nécessaires «entre les administrations fiscales et douanières» de différents pays ou «entre les services compétents en matière de sécurité sociale». Cette précision, qui ne semble concerner que l'instruction de cas particuliers, montre bien que cette dérogation ne peut être invoquée que si le transfert présente un intérêt pour les autorités d'un État membre de l'UE elles-mêmes, et non pas seulement pour une ou plusieurs autorités publiques du pays tiers.

Le groupe de travail insiste sur la nécessité ici aussi d'une interprétation stricte de la notion de «constatation, sauvegarde ou défense d'un droit en justice». Ainsi, par exemple, dans le cas où la société mère d'un groupe multinational, établie dans un pays tiers, serait poursuivie en justice par un de ses salariés, actuellement en poste dans une filiale européenne du groupe, la dérogation prévue par l'article 26, paragraphe 1, point d), semble autoriser cette société à requérir légalement de la filiale européenne qu'elle transfère certaines données relatives au salarié, dans la mesure où celles-ci sont nécessaires à sa défense.

En tout état de cause, cette dérogation ne peut justifier le transfert de l'intégralité des dossiers des salariés à la maison mère du groupe en raison de l'éventualité que de telles actions en justice pourraient être un jour intentées.

Cette dérogation ne pourra par ailleurs être appliquée que si les règles de procédure pénale ou civile applicables à ce type de situations internationales ont été respectées, notamment si elles découlent des dispositions des Conventions de La Haye

¹⁴ Avis 6/2002 précité.

du 18 mars 1970 (Convention sur «l'obtention de preuves»)¹⁵ et du 25 octobre 1980 (Convention sur «l'accès à la justice»)¹⁶.

2.5 TRANSFERT NECESSAIRE A LA SAUVEGARDE DE L'INTERET VITAL DE LA PERSONNE CONCERNEE (ARTICLE 26, PARAGRAPHE 1, POINT D))

Il va de soi que la dérogation prévue par l'article 26, paragraphe 1, point e), s'applique lorsque le transfert de données est motivé par une urgence médicale et que ces données sont considérées comme directement nécessaires à l'administration des soins requis.

Ainsi, par exemple, il doit être juridiquement possible de transférer des données, y compris certaines données personnelles, si la personne concernée est dans un état d'inconscience et a besoin de soins médicaux urgents et que seul son médecin traitant, établi dans un pays de l'UE, est à même de fournir ces données. En pareil cas, il serait absurde d'imposer une quelconque autre exigence pour garantir la légalité du transfert.

Le transfert doit être lié à l'intérêt individuel de la personne concernée et, lorsqu'il concerne des données médicales, être indispensable à l'établissement d'un diagnostic vital. Par conséquent, cette dérogation ne pourrait justifier le transfert de données personnelles à caractère médical à des responsables du traitement établis en dehors de l'UE, si le but du transfert n'est pas de traiter le cas particulier de la personne concernée mais, par exemple, d'effectuer des recherches médicales d'ordre général qui ne produiront des résultats qu'à terme. Dans ce cas, les transferts devraient reposer sur les exigences alternatives prévues par l'article 26, paragraphe 2, de la directive.

2.6 TRANSFERT INTERVENANT AU DEPART D'UN REGISTRE PUBLIC (ARTICLE 26 PARAGRAPHE 1, POINT F))

La dérogation prévue par l'article 26, paragraphe 1, point f), concerne les transferts qui interviennent «au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier».

Cette disposition de la directive est la conséquence logique du caractère public et librement consultable des registres en question. Si ces registres sont consultables par quiconque sur le territoire national ou par toute personne y ayant un intérêt légitime, il semble logique d'autoriser leur consultation par une personne établie dans un pays tiers.

Cette liberté de transfert de données ne peut toutefois pas être totale. Le considérant 58 de la directive précise en effet que «dans ce cas, un tel transfert ne devrait pas porter sur la totalité des données ni sur des catégories de données contenues dans ce registre». Il ne serait pas conforme à l'esprit de l'article 26, paragraphe 1, point f), que ce fondement juridique du transfert soit utilisé pour vider ces registres de leur contenu, avec le risque que des entités établies dans des pays tiers ne puissent, en fin de compte, les détourner de leur finalité initiale.

¹⁵ Convention de La Haye du 18 mars 1970 sur l'obtention de preuves à l'étranger en matière civile ou commerciale.

¹⁶ Convention de La Haye du 25 octobre 1980 tendant à faciliter l'accès international à la justice.

Le considérant 58 précise par ailleurs que «lorsqu'un registre est destiné à être consulté par des personnes qui ont un intérêt légitime, le transfert ne devrait pouvoir être effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires». On pourrait imaginer que cette dérogation puisse être utilisée, dans le respect des lois nationales, par une personne née dans un État membre de l'UE mais résidant dans un pays tiers, qui cherche à obtenir des extraits de ses actes d'état civil auprès sa commune de naissance afin de s'installer durablement dans son nouveau pays de résidence.

En tout état de cause, il conviendra de se reporter aux dispositions légales et réglementaires de l'État membre de l'UE où le registre a été établi, afin de vérifier si cette dérogation peut s'appliquer dans certains cas précis. Ces dispositions légales et réglementaires définiront en particulier les notions de «destiné à l'information du public» et d'«intérêt légitime» qui pourront ouvrir le recours à la dérogation.

3. CONCLUSION

Comme l'a précisé l'introduction, l'objet du présent document de travail est de fournir des indications pour l'interprétation des dérogations prévues par l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995.

Le groupe de travail maintient, dans le présent document, l'interprétation antérieure qu'il a exposée dans son document de travail WP12, selon laquelle toutes les dérogations énumérées à l'article 26, paragraphe 1, doivent être interprétées de manière stricte.

Cependant, dans un contexte marqué par l'accélération des transferts internationaux de données au cours des dernières années, dont témoigne à l'évidence l'activité quotidienne des autorités nationales de protection des données, le groupe de travail estime qu'il est nécessaire d'émettre des recommandations complémentaires au sujet de l'application de ces dispositions.

Ce faisant, le groupe de travail est particulièrement animé par le souci que les différentes bases juridiques qu'offre la directive pour les transferts internationaux de données soient utilisées de façon cohérente et, en tout état de cause, d'une manière ne portant pas atteinte au principe du niveau adéquat de protection consacré à l'article 25 de la directive.

À cet égard, le groupe de travail recommande que le présent document soit lu en liaison avec d'autres documents qu'il a précédemment adoptés dans le domaine des transferts internationaux de données et en particulier, le document WP74.

Le groupe de travail exprime le souhait que les responsables du traitement aient recours aux dérogations de l'article 26, paragraphe 1, dans le respect des recommandations énoncées dans le présent document.

Fait à Bruxelles, le

Pour le groupe de travail,
Le Président
Peter Schar