De quelques questions relatives à l'application de la directive "Données personnelles" n° 95/46 du 24 octobre 1995 au contexte d'Internet

Poullet, Yves

Published in:
Cahiers Lamy du Droit de l'Informatique

Publication date:
1997

Document Version
le PDF de l'éditeur

De quelques questions relatives à l'application de la directive « Données personnelles » nº 95/46 du 24 octobre 1995 au contexte de l'Internet

Notre propos n'est pas d'analyser de manière exhaustive les dispositions de la directive mais de signaler quelques conséquences et difficultés majeures de l'application de la directive au contexte de l'Internet (1). Ainsi, nous nous centrerons sur les trois points suivants :

- le premier est l'analyse de certaines définitions qui délimitent le champ d'application matériel de la directive ;
- le deuxième examine la portée territoriale de la directive ;
- le troisième s'attache à l'examen de principes fondamentaux de la directive relatifs aux limites des traitements de données.

I.– Le champ d'application matériel de la directive

L'analyse de deux notions retiendra notre attention.

La première est celle de « données à caractère personnel », c'est-à-dire, selon l'article 2 a, de données (2) qui se rapportent à une personne physique, identifiée ou identifiable. Cette notion trouve certainement à s'appliquer aux adresses électroniques personnalisées reprenant certains éléments relatifs à l'identité de leurs titulaires. Sans doute, s'appliquerait-elle également aux données de routage, aux empreintes électroniques laissées lors de l'utilisation de services présents sur le Net, dans la mesure où des moyens d'identification existent et sont à la portée du détenteur de la donnée (3).

Si l'extension de la notion pose peu de problème d'interprétation, on peut s'interroger sur sa pertinence dans le contexte de l'Internet. Un serveur peut, sans jamais chercher à connaître l'identité de l'utilisateur, disposer de nombreuses informations liées à l'adresse électronique voire IP de cet utilisateur et profiler ses services ou les services d'autrui en fonction du profil type de celui-ci. La simple donnée « adresse IP » ou « adresse électronique » ne mérite-t-elle pas dès lors protection, même s'il est prouvé que le serveur n'entend pas ou ne peut pas (4) identifier la personne disposant de cette adresse ? La question mérite attention. L'identification d'une personne se réfère-t-elle au nom de la personne ? Ne peut-on considérer qu'à travers une adresse et le profilage de l'utilisateur qui se cache derrière cette adresse, il s'agit également d'une identification de la personne ? Ou, sans se prononcer sur la nature personnelle ou non de la donnée, exiger, au vu des risques de réidentification, la démonstration par l'opérateur du site que son système présente les garanties « appropriées » de non identification des personnes concernées.

La seconde est celle de « traitement ». La notion de traitement est large et *vise toute opération depuis la collecte* jusqu'à la communication. L'application des dispositions de la directive à des opérations de simple consultation de site pose difficulté.

Faudra-t-il chaque fois, qu'il y a consultation de données nominatives sur Internet même sans stockage, ni copiage avertir les personnes concernées et leur ouvrir un droit d'accès à une donnée qui *in casu* n'est conservée que dans la mémoire humaine !

Une interprétation fondée sur le texte de la directive permet d'éviter une telle conséquence : au terme de l'article 2 b, la consultation n'est pas envisageable en tant que telle mais comme un élément d'un traitement, c'est-à-dire comme la possibilité offerte par le traitement de laisser consulter les données (5).

II.– Le champ d'application territorial de la directive

A.– Le champ d'application « normal » de la directive

La directive est applicable à tout traitement dont le responsable est localisé sur le territoire d'un des pays de l'Union européenne (6). Un tel critère de rattachement est particulièrement idoine en matière de protection des données. Dans la mesure où un site peut être « logé » sur n'importe quel ordinateur situé sur le réseau, le critère du responsable c'est-à-dire de celui qui définit les finalités et les moyens du traitement présente plus de stabilité (7).

La difficulté demeure lorsque le responsable et son adresse ne peuvent être identifiés (8). Une solution pourrait être alors de rendre responsable celui qui assure la maintenance du site en question en localisant la machine où est situé le site (9).

La localisation du responsable soulève d'autres difficultés : une simple adresse électronique est rarement parlante quant à la localisation d'un site (10). En outre, qui est responsable d'un forum de discussion ? Si on considère que c'est le modérateur, faut-il se fixer en ce qui concerne la loi acceptable, à l'adresse de son établissement ?

B.– La portée internationale de la directive

Selon l'article 4 c) de la directive, le droit national pris en application de la directive s'applique : « *lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire dudit État membre* ». L'article 4.2. ajoute que l'applicabilité du droit national entraîne l'obligation pour le responsable de désigner un représentant établi sur le territoire de l'État membre (11).

Le critère de rattachement affirmé par le texte est donc le « recours » à des moyens automatisés ou non situés sur le territoire de l'Union européenne. La notion est vague.

Prise au sens large, elle consacrerait des hypothèses où la collecte des informations opérée par exemple en Belgique est suivie par un transfert des données vers l'étranger pour y

être traitée par exemple à meilleur prix mais également l'interrogation d'une banque de données sise en Belgique, dans la mesure où interrogeant une boîte aux lettres tenue à sa disposition en Europe par une agence de voyage, il prend connaissance de messages EDI qui lui sont destinés. Appliquée à Internet, une telle interprétation permettrait de considérer que toute personne qui interroge un site européen et télédécharge des données nominatives à partir de son interrogation recourt à des moyens automatisés situés sur le territoire de l'Union Européenne et se voit donc appliquée la directive.

Bref, l'interprétation large de la notion de « recourir » aboutirait à décréter que la quasi totalité des flux transfrontières générés par Internet amènerait le destinataire des flux à tomber sous le champ d'application de la directive. Point ne serait besoin alors des dispositions des articles 25 et 26 de la directive, puisqu'en toute hypothèse la directive serait applicable.

Lors d'une analyse récente de l'application de la directive à Internet, M.-H. Boulanger et C. de Terwangne (12) ont proposé une autre interprétation qualifiée de « téléologique » du critère de rattachement proposé par l'article 4.1.C). Nous en reproduisons le texte : « La *ratio legis* de cet article se résume clairement dans la volonté d'éviter que les individus se trouvent dépourvus de toute protection, en particulier du fait d'un contournement de la législation. Le souci des auteurs du texte est donc d'assurer une protection à ceux qui doivent normalement en bénéficier sous l'égide de la directive, même en dehors des frontières communautaires.

C'est par une lecture combinée de l'article 4.1.c et des articles 25 et 26 qui régissent les flux transfrontières vers les Etats tiers qu'une définition rationnelle de l'applicabilité de la directive pourra être dégagée.

On peut, en effet, considérer qu'une première réponse à la préoccupation des auteurs de la directive est donnée par l'instauration d'un régime protecteur en matière de flux transfrontières de données vers les pays tiers à la Communautés. Dans le cadre de la réglementation de ces flux, les exigences édictées par la loi européenne s'imposent à tous les acteurs qui effectuent des opérations sur des données fournies à l'étranger en provenance de l'Union est exigée ».

On peut, en effet, considérer qu'une première réponse à la préoccupation des auteurs de la directive est donnée par l'instauration d'un régime protecteur en matière de flux transfrontières de données vers les pays tiers à la Communauté. Dans le cadre de la réglementation de ces flux, les exigences édictées par la loi européenne s'imposent à tous les acteurs qui effectuent des opérations sur des données fournies à l'étranger en provenance de l'Union est exigée ».

La réponse contenue dans l'article 4.1.c. vise à couvrir, quant à elle, les situations dans lesquelles les sujets des données se voient privés, par une manœuvre artificielle, du bénéfice de la protection de l'ensemble de la directive, et les situations échappant à toute protection, même celle instaurée en matière de flux transfrontières. Dans ce sens, deux catégories de situations entrent, selon nous, dans le champ de l'article 4.1.c. :

- celle précisément où un responsable de traitement cherche délibérément à contourner la directive et, pour ce faire, délocalise son établissement vers un pays tiers, tout en faisant usage de moyens localisés sur le territoire communautaire pour réaliser son traitement. Par exemple, le cas d'un serveur d'annuaires téléphoniques reprenant les abonnés italiens et dont la cible commerciale est purement ou en tout cas majoritairement européenne mais qui pour éviter les réglementations européennes s'installerait au Maroc ;
- celle où le flux est le fait exclusif d'un responsable localisé dans un pays tiers. A notre avis, cette situation vise les collectes de données personnelles réalisées par le biais de cookies introduites dans le système d'informations de l'utilisateur et à son insu.
  Dans un tel cas, le responsable du site « recourt » à des moyens électronique situés dans le pays de l'utilisateur (13).

Elle pourrait également viser une collecte opérée à partir de l'étranger par le biais d'un logiciel qui visiterait l'ensemble des forums de discussions mis en place par des serveurs européens et d'y repérer les interventions de telle ou telle personne afin de constituer son profil de personnalité.

Par contre, il apparaît peu raisonnable de considérer que suite à l'envoi conscient par un utilisateur d'un message à un site hors Europe, ce site tombe sous le champ d'application de la directive. Dans un tel cas, il y a transmission de données nominatives vers un pays tiers et les dispositions des articles 25 et 26 s'appliqueront.

En conclusion, l'article 4.1.c) viserait des hypothèses exceptionnelles soit celle où la localisation du responsable est anormale au regard de son autorité orientée vers l'Union européenne et déterminée par des données en provenance de celle-ci, soit celle où est déjouée la protection offerte par la réglementation des flux transfrontières dans la mesure où ce flux est généré par la seule activité de la personne située à l'étranger sans qu'il y ait à proprement parler communication, c'est-à-dire action consciente de transfert de données, d'un responsable de traitement situé dans le territoire de l'Union européenne.

C.– Les flux transfrontières

1. Le principe : la nécessité d'une protection adéquate (14)

En vertu de l'article 25.1. de la directive, « *les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat* ». Le principe est donc l'interdiction du transfert, sauf à démontrer le caractère adéquat de la protection offerte dans le pays tiers.

La directive précise ensuite en son article 25.2 que l'appréciation (15) du caractère adéquat de la protection du pays tiers doit tenir compte de « *toutes les circonstances relatives à un transfert ou à une catégorie de transfert* » et en particulier de différents facteurs, dont certains sont fonction du transfert considéré, tels la nature des données, la finalité et la durée des traitements, les pays d'origine et de destination, et certains concernant le niveau de protection dans le pays tiers, comme les règles de droit générales ou sectorielles en vigueur ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

Au-delà de ces réflexions, la notion de « *protection adéquate* » conduit à une approche – qui, à la lecture du texte de l'article 25, se caractérise comme suit :

- une approche au cas par cas (16), c'est-à-dire que la situation de la protection de données dans un pays tiers est évaluée « par rapport » à un transfert déterminé ou une catégorie de transferts. L'instrument méthodologique doit caractériser de manière précise le cas visé ;
- une approche souple et ouverte puisque selon le libellé même de l'article 25.2 l'évaluation doit pou-

voir tenir compte à la fois des particularités propres et évolutives des divers flux transfrontières mais également des solutions diverses et évolutives que chaque État, voire chaque responsable des données, peut apporter, l'article 25, 2 étant purement indicatif à ce propos ;

- une approche fonctionnelle, c'est-à-dire que la protection s'évalue tant par rapport aux risques d'atteinte à la protection des données, risques générés par le flux en question, que par rapport aux mesures spécifiques ou générales mises en place par le responsable des données dans le pays tiers pour pallier ces risques.

L'évaluation de ces mesures doit se faire sans *a priori* : il ne peut être question d'imposer les mécanismes européens mis en place selon la directive (pas d'impérialisme européen) mais bien d'apprécier dans quelle mesure les objectifs de protection poursuivis par la directive sont rencontrés, de façon originale ou non par un pays tiers. En ce sens, la notion de protection adéquate ne représente en aucune manière un affaiblissement de la protection des données des personnes protégées au départ de la directive. Au contraire, elle crée pour l'évaluateur la nécessité, tout en ne perdant pas de vue les exigences qui fondent selon la directive le besoin de protection, de prendre en considération les adaptations originales des modalités de cette protection, adaptations proposées par les pays tiers. Il s'agit de rechercher s'il y a « similarité fonctionnelle (17) ».

Quelques remarques liminaires s'imposent d'emblée au sujet de la notion d'« adéquation », que d'aucuns ont opposé à celle d'« équivalence » (18).

Tout d'abord, cette notion suppose sans doute un référent (qui permette de répondre à la question : « par rapport à quoi la protection doit-elle être adéquate » ?). Or, ce référent n'est pas défini comme tel par la directive. Il n'existe pas de système de référence déterminé par rapport auquel on puisse évaluer, la protection du pays tiers.

Ensuite, on note que, si les critères énoncés par l'article 25.2 constituent de précieuses indications quant aux éléments à prendre en compte pour évaluer l'adéquation de la protection du pays tiers, ils ne constituent pas une liste exhaustive (l'article 25.2 énonce qu'il faut « en particulier » prendre en considération tel ou tel élément). On peut prendre en compte bien d'autres facteurs pour affiner cette analyse, que ces facteurs soient relatifs au flux considéré ou à la protection existant dans le pays tiers.

Troisièmement, le contenu de ces éléments n'est pas défini : si par exemple on sait qu'il faut prendre en compte la durée des traitements, la directive n'indique pas plus avant ce qui serait une durée acceptable ou non. De même, le texte communautaire ne détaille pas ce que devraient être le « contenu minimum » d'une législation ou encore ses conditions d'application, pour considérer qu'elle assure un niveau adéquat de protection.

On ajoutera que certains éléments énoncés se réfèrent aux caractéristiques du flux et désignent des facteurs de risques, alors que d'autres désignent la qualité des instruments de protection mis en place dans le pays tiers.

Enfin, à propos des instruments de protection mis en place, l'article 25 se réfère non seulement aux normes issues de l'autorité publique qu'elles soient générales ou sectorielles (19) mais également à des codes de conduite (20) voire à des mesures techniques pourvu que ces instruments soient « respectés ». Ainsi l'autorité de protection sera plus attentive à l'effectivité d'un instrument, qu'à sa nature : ce qui importe, c'est qu'elle soit convaincue que l'instrument – même s'il s'agit d'une simple « *Company Privacy Policy* » – soit largement diffusé parmi les personnes concernées et les responsables des fichiers et puisse faire l'objet de recours des premiers vis-à-vis des seconds en cas de non-respect par ceux-ci.

L'article 25, alinéa 1er et alinéa 2 consacre, nous l'avons dit, une approche au cas par cas, flux par flux ou catégorie de flux par catégorie de flux. Une telle analyse est évidemment lourde pour les Etats membres et les articles 25.4 et 25.6 mentionnent deux possibilités pour la Commission de leur simplifier le travail. Il s'agit de constater « conformément » à la procédure prévue à l'article 31, 2 qu'« *un pays tiers assure ou n'assure pas un niveau de protection adéquat* ». En d'autres termes, ces paragraphes permettent la constitution de « white » ou de « black » lists, décision valable pour des catégories de transferts, pour un secteur, voire pour l'ensemble des flux vers un pays tiers (21).

2. *Les exceptions*

La directive, « *sous réserve de dispositions contraires de leur droit national régissant des cas particuliers* » (22), édicte certaines exceptions au principe de l'article 25 et autorise ainsi des transferts de données à caractère personnel vers des pays n'offrant pas un niveau de protection adéquat.

Deux types d'exceptions sont prévus : le premier vise certaines catégories de flux ; le second vise la substitution à un mode adéquat de protection, d'un mode « *ad hoc* » de protection : le contrat.

À propos de la première catégorie d'exceptions, l'article 26.1 vise notamment les hypothèses où la personne concernée a indubitablement donné son consentement à l'opération de transfert (article 26.1a).

On ne peut parler de véritable consentement que si celui-ci est « éclairé » c'est-à-dire si la personne concernée a conscience qu'il s'agit bien d'un flux transfrontalier, connaît le pays de destination des informations qu'elle transmet et réalise que ce pays n'assure pas un niveau de protection adéquat des données. Cette première exception se révélera utile dans le cadre d'Internet dans la mesure où le consentement pourra être demandé et obtenu directement *via* le réseau. D'autres exceptions existent. Elles reprennent en gros les hypothèses prévues par l'article 7 de la directive pour légitimer un traitement.

Tantôt le transfert est nécessaire à l'exécution d'un contrat ou à l'exécution de mesures précontractuelles, soit entre la personne concernée et le responsable du traitement soit entre le responsable du traitement et un tiers dans l'intérêt de la personne concernée (23). Tantôt le transfert sert à la sauvegarde d'un intérêt vital ou d'intérêt public important ou s'opère dans le cadre d'une action en justice (24).

La seconde catégorie d'exceptions substitue à des modes adéquats de protection, ceux palliatifs envisagés par le responsable dans le cadre d'un flux ou de plusieurs flux pour garantir le respect de la protection des données.

Les clauses contractuelles en particulier (25) sont visées. Ainsi, si le secteur marketing d'un pays tiers n'offre pas de protection adéquate aux données originairement protégées par la directive, une entreprise (ou l'association des sociétés de marketing) peut prendre dans le cadre des contrats couvrant les flux transfrontières en provenance d'Europe, des engagements supplémentaires, par exemple limitant les finalités de réutilisation des données, ouvrant le droit d'opposition et finalement permettant à une autorité de protection des données d'inspecter leurs traitements (26).

III.– De quelques principes de base de la directive

Internet représente à la fois un outil de collecte d'informations mais également de communication entre la personne concernée et le responsable du traitement. Cette double fonction présente dans un même média permet de rendre plus effectives certains dispositions de la directive. On songe en particulier à la manière dont le principe de transparence, les droits d'accès, de correction pourraient s'exercer *via* Internet et à moindre coût. Au-delà, la configuration des écrans pourrait permettre à l'internaute de connaître à tout moment l'identité du responsable, les finalités poursuivies par celui-ci voire, *via* un lien html, les dispositions réglementaires ou autoréglementaires que le responsable s'engage à suivre (27).

L'interactivité du média ouvre d'autres possibilités encore, possibilité de déterminer les utilisations de données, auxquelles l'utilisateur consent, et ce en cochant des cases apparaissant à l'écran avant la collecte des données, possibilité d'exercer *a priori* son droit d'opposition, etc.

Le consentement reçoit, dans le contexte d'Internet, une portée et une efficacité nouvelle. On pourrait être tenté d'y voir une base de légitimité suffisante pour les traitements de données collectées via Internet. En ce sens, on relève une disposition d'un projet de loi allemand qui considère le consentement comme fondement suffisant d'un traitement effectué *on line* suite à l'utilisation d'un service disponible.

Nous pouvons difficilement accepter un tel raisonnement. Outre que le consentement risque de ne point être libre et éclairé, il ne dispense pas d'un examen de la légitimité du traitement (28). Certes, cet examen se fondera sur une appréciation marginale dans la mesure où le consentement au traitement crée une forte présomption mais une telle présomption pourrait céder devant une interdiction de l'État relative au traitement de certaines données (29) ou de certains traitements (30). Par ailleurs, une action *a posteriori* des autorités judiciaires ou de contrôle pourrait considérer le traitement pourtant consenti comme illégitime.

Le principe de la collecte et du traitement loyal s'applique aux traitement réalisés via Internet. L'article 6.1 a de la directive qui exige que la collecte et l'utilisation de données soient faites de manière loyale exclut des pratiques comme celles dénoncées dans la première section à propos des traitements invisibles. « *Personal Data may only be collected in a transparent way* » (31).

On ajoutera enfin que selon l'article 6.1 b l'utilisation des données doit être « compatible » avec la ou les finalités annoncés lors de la collecte des données, c'est-à-dire rentrer dans le champ des utilisateurs raisonnablement attendus par la personne concernée à la lecture de finalités annoncés par le responsable du traitement.

Quelques exemples illustrent cette notion : en participant à un forum public de discussion relatif à la cryptographie, une personne peut s'attendre à ce que des invitations lui soient envoyées à propos de conférences ou séminaires en la matière ; par contre le consommateur qui visite le site d'un supermarché sur Internet ne peut raisonnablement pas s'attendre à ce qu'une firme tierce sur la base de l'analyse de son profil de personnalité lui propose l'achat d'ouvrages ou la participation à tel ou tel voyage, comme cela pourrait être le cas si les deux entreprises participent à un système commun d'analyse du comportement de l'utilisateur comme « double click ».

L'Internaute qui accède au réseau *via* un fournisseur d'accès peut raisonnablement s'attendre à ce que ses données de connexion soient utilisées par le fournisseur d'accès pour que ce dernier lui propose des conditions spéciales mais non pour communication à des serveurs avec lesquels ce fournisseur entretient des relations privilégiées.

Yves POULLET

Directeur du CRID,

Professeur à la Faculté de Droit et au DES en Droit et Gestion des Technologies de l'Information et de la Communication de Namur–FUNDP

Notes

(1) Le lecteur se référera pour ce faire à l'analyse plus complète proposée par C. de Terwangne et S. Louveaux, *Data Protection and on line networks*, *Computer Law and Security Report*, 1997, à paraître. Certaines idées exposées ci-dessous sont reprises de l'analyse proposée par ces auteurs.

(2) ... qu'il s'agit de textes, de sons ou d'images. Cette précision est importante dans la mesure où Internet devient de plus en plus un réseau multimédia (ex. mise sur le réseau d'un curriculum vitae avec photo du candidat).

(3) *Cf.* le considérant nº 26 : « ... pour 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 ».

(4) Le considérant nº 26 souligne que les moyens doivent être susceptibles d'être mis en œuvre et non être effectivement mis en œuvre.

(5) À propos de cette interprétation, M.-H. Boulanger, C. de Terwangne, *Internet et le respect de la vie privée*, *in Internet face au droit* ; E. Montero, *Cahier du CRID*, nº 12, Bruxelles, *éd. Story Scientia*, 1997, p. 211.

(6) Sans doute, faudrait-il prévoir comme le font les réglementations de protection des consommateurs en matière de ventes à distance, l'obligation pour tout site d'identifier clairement le responsable du site, son adresse et sans doute les finalités de la collecte d'informations personnelles.

(7) *Cf.* à ce propos, la définition donnée par l'article 2 d de la directive. L'article 4.1 a) de la directive ajoute que si le responsable dispose de plusieurs établissements sur le territoire de plusieurs pays de l'Union, il doit observer les droits nationaux des divers pays des établissements. À notre avis, le fait que le site d'un responsable est consultable de divers pays de l'Union Européenne ne conduit pas à affirmer la pluralité d'établissements. La notion d'établissement se réfère (considérant nº 11) à une installation stable, ce qui n'est pas le cas ici...

(8) Sans doute, faudrait-il prévoir comme le font les réglementations de protection des consommateurs en matière de ventes à distance, l'obligation pour tout site d'identifier clairement le responsable du site.

(9) On est conscient du fait que cette machine peut être une simple boîte postale électronique où est hébergé temporairement le site.

(10) À ce propos, M.-H. Boulanger, C. de Terwangne, précité, p. 201.

(11) Auprès duquel s'exerceront notamment les droits d'accès, d'opposition, et de rectification.

(12) M.-H. Boulanger, C. de Terwangne, précité, p. 202. Les auteurs se réfèrent également à la lecture du considérant nº 20 et à l'exposé des motifs de la première proposition de directive émanant du Conseil (Proposition du 15 octobre 1992, COM(92) 422 final – SYN 287, p. 13).

(13) M.-H. Boulanger, C. de Terwangne, précité, p. 210 considèrent que le même raisonnement s'applique dans le cas de l'enregistrement de données de routage, c'est-à-dire selon les auteurs dans le cas de flux actifs cachés. Flux actifs dans la mesure où ils sont initiés par une action de la personne concernée.

(14) Sur l'étude de cette notion, B. Havelange, Y. Poullet, (avec la collaboration de M.-H. Boulanger, H. Burkert, C. de Terwangne, A. Lefebvre), *Élaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel*, Exec. Summary, Étude réalisée pour la Commission des Communautés européennes, février 1997, à paraître.

(15) De qui relèvera l'appréciation du caractère adéquat ? Quel rôle joueront dans cette procédure les autorités nationale de protection des données ?

(16) Par opposition à une approche législative qui se fonderait sur une comparaison des textes.

(17) La « similarité fonctionnelle » implique que l'on recherche non la transposition pure et simple des principes et systèmes de protection européens dans les pays tiers, mais bien la présence de tout élément remplissant les fonctions recherchées, même si lesdits éléments doivent être d'une nature différente de ceux que l'on connaît en Europe. Elle permet sans doute un meilleur respect des structures et des caractéristiques juridiques locales qu'un requis de protection équivalente, qui exige une similarité complète, législative en tout cas.

(18) La notion de protection équivalente est utilisée par la Convention du Conseil de l'Europe, dite Convention nº 108 en son article 12. Cet article met à charge d'une partie contractante une obligation de permettre les flux vers les autres États partie à la même convention si cet État assure une protection équivalente. On notera que la notion d'équivalence de protection ne règle que les flux entre pays ayant ratifié la Convention du Conseil de l'Europe et non vers les pays tiers.

À propos de cette différence, A. Bourlond, Y. Poullet, *Flux transfrontières de données à caractère personnel, position de la proposition de directive européenne face à celle de la convention 108 du Conseil de l'Europe*, *DIT* 1991, nº 2, p. 58 et s.

(19) Ainsi, une législation sur le secret médical pourrait garantir adéquatement dans le secteur médical, la protection des données.

(20) La *Canadian Standard Association* a établi un code de conduite modèle en matière de respect de la vie privée qui prévoit des mécanismes originaux de certification pour les entreprises par des organismes agréés et des recours possibles. À propos de ce modèle, C. Bennett, Privacy Codes, *Privacy Standards and Privacy Laws : the instruments for Data Protection and what they can achieve*, *Paper presented at Visions for Privacy*, Victoria, British Columbia; 9-11 mai 1996.

(21) Analyse au cas par cas et analyse globale : les deux types d'analyses ne sont pas contradictoires. L'analyse globale suivra le plus souvent une série d'évaluations au cas par cas, éventuellement pratiquées par différents États membres ; elle pourrait également se déduire d'un système de protection générale des données dont le contenu, le contexte et l'application désignent à coup sûr comme adéquate ou inadéquate la protection offerte par les pays tiers.

(22) « Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur national régissant des cas particuliers, les États membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat (...) peut être effectué (...) (Article 26.1). « Les États membres peuvent donc, par des dispositions régissant des cas particuliers, refuser que l'une ou l'autre exception s'applique à ces cas. On pense dans un premier temps aux situations mettant en jeu des données sensibles, médicales ou judiciaires. Mais la particularité des cas retenus peut être plus large et consister non plus dans le caractère sensible des données mais, par exemple, dans la nature du réseau – ouvert ou fermé – utilisé. On peut donc imaginer qu'un État membre soit plus strict qu'un autre en matière d'exceptions appliquées à l'utilisation d'un réseau Internet » (M.-H. Boulanger, C. de Terwangne, *Internet et le respect de la vie*

privée, in Internet face au droit ; E. Montero, *Cahiers du CRID*, n° 12, Bruxelles, *éd. Story Scientia*, 1997, p. 211). L'interprétation donnée par les auteurs cités est ainsi large. La notion de « cas particulier » pourrait s'interpréter comme laissant seulement la possibilité pour l'autorité nationale d'intervenir pour un flux déterminé et de déroger exceptionnellement et non par catégorie aux différentes hypothèses prévues par l'article 26.

(23) Ainsi par exemple un service de réservation aérienne transmettra à des agences locales de voyage le nom des voyageurs désirant réserver un hôtel.

(24) L'article 26.1 6) ajoute le cas d'un transfert à partir d'un registre public « destiné réglementairement à l'information au public et ouvert à la consultation » (ainsi, par ex., le registre du commerce).

(25) À l'appui d'un contrat, des mesures techniques *ad hoc* pourraient également être envisagées pour constituer une garantie suffisante. Sur les contrats, comme modèle supplétif d'assurer une protection équivalente ou adéquate dans les flux transfrontières, C.-M. Pitrat, *Clauses modèles pour les flux transfrontières de données ou comment assurer une protection équivalente*, *DIT* 1993, n° 1, p. 46 à 52 ; L. Early, *Securing equivalent protection among nations in the context of TBDF : a possible role for contract law*, *DIT* 1990, n° 4, p. 10 et s. Le lecteur trouvera dans ces écrits des références aux clauses modèles élaborées conjointement par le Conseil de l'Europe et la CCI (Strasbourg, 2 novembre 1992, TPD(92) 7 revised).

(26) À propos de ce second type d'exception, une autorisation de l'État membre sera nécessaire. Elle supposera le caractère « suffisant » des garanties offertes. L'État membre devra informer la Commission de telles autorisations et des oppositions exprimées par d'autres États membres seront possibles. On souligne, à ce propos, le rôle important joué par la Commission qui peut, après délibération des représentants des États membres, imposer une décision aux États membres seront possibles. On souligne à ce propos, le rôle important joué par la Commission qui peut, après délibération des représentants des États membres, imposer une décision aux États membres, soit l'acceptation de telles mesures palliatives, soit leur rejet ou la proposition de mesures supplémentaires.

(27) On pourrait même songer à voir apparaître à l'écran les données relatives au traitement qui sont consignées dans le registre accessible au public, tenu par l'autorité de contrôle.

(28) Ainsi, on peut douter de la liberté de consentement du chercheur d'emploi, appelé à donner certaines données de son passé par un serveur ayant créé une banque de données de recherches d'emploi.

(29) La directive prévoit expressément la possibilité pour l'État de prévoir des exceptions en matière de données (art. 8, 1 a). Le Budapest-Berlin Memorandum interdit la publication d'avis de recherche policiers sur Internet vu le manque de sécurité des problèmes d'authentification et les possibilités de manipulation des images.

(30) Ainsi, en matière de vidéotex, les traitements d'analyse psychologique du comportement de l'utilisateur, lors de son utilisation de jeux vidéo avaient été condamnés.

De même, les câblo-opérateurs américains se sont vus interdire sauf pour finalités d'analyse du marché l'enregistrement des choix de programmes réalisés par un spectateur. Par analogie, ne pourrait-on interdire ce type de traitement aux fournisseurs d'accès.

(31) C'est le Guidance 2 affirmé par le Budapest-Berlin Memorandum déjà cité.