

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Flux transfrontières de données

Poullet, Yves

Published in:
Droit & technologie

Publication date:
2003

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Poullet, Y 2003, 'Flux transfrontières de données: vie privée et groupes d'entreprises. A propos d'une opinion récente du Groupe de travail "Article 29" sur la protection des données' *Droit & technologie*. <<http://www.droit-technologie.org>>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



Présente :

**Flux transfrontières de données,
Vie privée et Groupes d'entreprises
A propos d'un opinion récente du Groupe de travail
« Article 29 » sur la protection des données**

Colloque de l'AEBDF
Monaco-Octobre 2003
« Les centres financiers à l'épreuve du
droit européen et du droit international »

Par

Yves Poulet

Doyen de la faculté de droit de Namur
Directeur du Centre de recherche Informatique et Droit
www.crid.ac.be
yves.poulet@fundp.ac.be

Date de mise en ligne : 26 décembre 2003

Flux transfrontières de données, Vie privée et Groupes d'entreprises

A propos d'une opinion récente du Groupe de travail « Article 29 » sur la protection des données

Colloque de l'AEBDF
Monaco-Octobre 2003
« Les centres financiers à l'épreuve du
droit européen et du droit international »

Yves Poulet
Doyen de la faculté de droit de
Namur
Directeur du Centre de
recherche Informatique et Droit
<http://www.crid.ac.be>
yves.poulet@fundp.ac.be

1. Le 3 juin de cette année, le groupe de travail dit de « l'article 29 » sur la protection des données¹ a adopté le document de travail : « 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 ».

Le document entend résoudre la question délicate de la circulation des données protégées par la directive 95/46/CE au sein de groupes d'entreprises dont la dimension dépasse les frontières de l'Union européenne. La solution originale proposée se justifie par les particularités de la situation des multinationales, qui peuvent difficilement se satisfaire des solutions proposées dans ou sur base de la directive. Cette solution originale présente une réelle continuité avec les principaux traits des solutions déjà définies ; elle entend accentuer une reconnaissance de la valeur de l'autorégulation, comme mode normatif susceptible d'offrir une protection adéquate des données.

2. Avant d'aborder l'analyse de la solution proposée (TITRE II), il importe d'en situer le double contexte (TITRE I) : celui économique décrit la réalité des flux transfrontières au sein des groupes d'entreprises (article 1), celui juridique situe les diverses solutions jusqu'alors adoptées et confire leur inadéquation dans le cas précis (article 2).

I Le double contexte

Chapitre I : Le contexte économique : les groupes de sociétés²

3. La globalisation des marchés en même temps que les stratégies de regroupement d'entreprises expliquent le développement des groupes d'entreprises et la multiplication des flux au sein de ces groupes. Le phénomène certes n'est pas neuf mais prend une dimension nouvelle ; ainsi, la mobilité requise des compétences humaines au sein de ces groupes justifie sinon la constitution de base de données centrales relatives au personnel, au moins des possibilités de transfert de données relatives à ces derniers. Les spécialisations des établissements au sein de ces groupes, la répartition des marchés exigent le partage d'informations quant aux clients tantôt afin de leur fournir un service global, tantôt afin de leur proposer des services complémentaires. Ainsi, la banque établie en Europe pourra servir

¹ C'est en effet l'article 29 de la directive 95/46/CE qui crée cet organe consultatif indépendant, composé de représentants des différentes autorités de contrôle nationales. Le lecteur consultera les résultats des travaux du Groupe de l'article 29 sur le site www.europa.eu/int/comm/privacy.

² Sur la notion « floue » de « groupe de sociétés », lire notamment C. Hannoun, *Le droit et les groupes de sociétés*, LGDJ, Paris, 1991. Cf. la tentative de définition de l'Union européenne : « Le groupe y est défini selon deux traits principaux : l'état de dépendance de la filiale, que peut traduire la participation en capital ou de simples éléments de fait ; et l'unité de direction des sociétés membres du groupe » (C. Hannoun, *op.cit.*, p. 4). Voir également, les remarques de A. Benoît-Moury, *Entreprises et phénomène associatif*, in *La coopération entre entreprises*, ABJE, Bruylant, Kluwer, 1993, p. 464 qui évoque des notions légales comme « action de concert » et « contrôle conjoint ». L'auteur conclut (p. 465) : « La pratique a précédé la norme juridique, la créativité et l'imagination des juristes ont fait face au vide législatif ou ont permis des constructions originales adaptées aux nécessités économiques ou aux spécificités des situations. ». Cf. plus récemment l'étude de E. Wymeersch, *Comment le droit pourrait aborder certains groupes de sociétés ?*, Mélanges P. van Ommeslaghe, 2002, p ;703 et ss.

de guichet unique pour les services bancaires ou autres offerts par les autres membres du groupe. Ainsi, se partagera-t-on volontiers au sein du groupe des fichiers marketing.

La notion de « groupe d'entreprises » est difficile à définir et le groupe 29 ne s'y risque pas. Sans doute, soulignera-t-on que les relations entre membres du groupe peuvent être plus ou moins distendues, plus ou moins hiérarchisées. Entre la simple entente entre entreprises autonomes dans leurs directions et stratégies et la multinationale entièrement pilotée par la maison mère, il y a peu de ressemblances et, sans doute, les flux seront tant quantitativement que qualitativement plus importants dans le second cas que le premier. Nous reviendrons sur ce point qui n'est pas sans conséquence sur la recevabilité des solutions proposées.

Il va en effet de soi qu'une structure fortement hiérarchisée dispose d'autres moyens de pression et de contrainte pour faire respecter les décisions prises en son sein, et ce, à l'inverse d'une structure plus éclatée sans unité de direction et de stratégie³. Nous aurons l'occasion de montrer combien cette considération est relevée par le groupe dit de l'article 29.

4. Une autre caractéristique du groupe est sa dimension évolutive : le groupe d'entreprises peut s'étendre à de nouveaux territoires (implantation de nouvelles filiales ou succursales, joint ventures avec des entreprises, etc.) ou, à l'inverse, se restreindre en cas d'abandon ou de ventes d'activités ou de retrait de certains pays. L'existence de configurations géographiquement variables dans le temps crée indéniablement une difficulté : là où les flux n'étaient envisagés que vers certains pays, des décisions d'investissement ou de délocalisation peuvent amener des implantations nouvelles non prévues au départ. Dès lors, en termes de réglementation de protection des données, il est difficile de prendre en considération la situation existante dans des pays dont la liste n'est point close.

5. A cette variabilité géographique du groupe d'entreprises, s'ajoute celle plus importante des flux intra-groupes, dans la mesure où ceux-ci entendent profiter au maximum de leurs multiples implantations, des réglementations existantes dans les divers pays et des stratégies mouvantes de concertation entre les diverses unités pour modifier, intensifier, rediriger les flux d'informations y compris nominatives entre ces unités. Ainsi, peuvent-elles décider de centraliser les informations relatives au personnel pour accroître la mobilité de celui-ci, pour mener des politiques cohérentes voire uniformes de promotion ou de contrôle des travailleurs. Elles conduiront des stratégies de marketing à direction d'un pays à partir de tel ou tel pays selon les ressources qu'elles peuvent y trouver et les relations avec les fournisseurs hier décentralisées, peuvent demain se trouver centralisées. Bref, la dynamique changeante du groupe influe profondément sur la structure, la quantité et la qualité des flux.

Une dernière considération a trait à l'ancrage européen du groupe d'entreprises. Plus cet ancrage est important, plus la culture réglementaire européenne peut facilement dominer les

³ Sur cette diversité des montages et la difficulté de distinguer nettement les hypothèses, lire M.Coipel, Lettre de patronage et droit des sociétés, in Les lettres de patronage, Faculté de droit de Namur – Feduci, Namur Paris, 1984, p.201 et ss. : « Les deux ensembles que constituent, d'une part, les sociétés dominantes/dépendantes et, d'autre part, les groupes de sociétés se recoupent, certes, mais ne se recouvrent pas entièrement. Il se peut qu'un lien de dépendance existe entre deux ou plusieurs sociétés sans qu'il y ait groupe à défaut de direction unique. En effet, il y a lien de dépendance même si la société dominante n'utilise pas effectivement de son pouvoir alors que la direction unique doit être effective pour qu'il y ait groupe. D'autre part il se peut qu'une société exerce effectivement une influence dominante sur la conduite des affaires d'une autre société sans que pour autant, les sociétés soient gérées quant à leurs fonctions essentielles, selon des objectifs et des conceptions identiques : la direction unique fait alors défaut. »

opérations des entre membres du groupe. On conçoit que pour un groupe dominé de l'extérieur de l'Europe, que ce soit du Japon ou des Etats-Unis, les principes mêmes de la directive européenne de protection des données à caractère personnel seront difficilement intégrés dans les stratégies décidées à partir de la maison mère. Le faible ancrage des activités d'une multinationale aura une seconde conséquence : les données nominatives collectées en Europe représenteront un faible pourcentage des données traitées par la multinationale et on peut craindre dès lors que les autorités du groupe aient quelque difficulté à justifier de précautions ou garanties liées à la provenance de données minoritaires. On peut craindre que le groupe ne leur oppose que le traitement de telles données conduit, vu les exigences européennes, à assortir le traitement de l'ensemble des données à des garanties supplémentaires, coûteuses et non exigées légalement pour les données qui constituent le contenu majoritaire des traitements opérés par le groupe.

Chapitre II : Le contexte juridique : les flux transfrontières de données et la directive 95/46/CE⁴

6. On sait que la directive contient diverses dispositions relatives aux flux : la principale est certes l'article 25 qui affirme le principe de la protection adéquate.

En bref, les flux transfrontières de données à caractère personnel protégés par la directive est interdit vers des pays tiers sauf à démontrer que l'entreprise, le secteur, le pays offre une protection adéquate eu égard aux risques spécifiques d'atteinte à la protection des données générées par le flux ou le type de flux en question⁵. La protection est offerte ici par l'environnement « normatif » externe dans lequel s'opère le flux. La Commission, sur base de l'article 25.6 de la directive a ainsi considéré divers systèmes législatifs⁶ ou

⁴ Pour un exposé complet en la matière, le lecteur se référera aux articles suivants : B. Havelange et A-C Lacoste, Les flux transfrontières de données à caractère personnel en droit européen, *JTDE*, 2001, p. 240 et ss. ; Y. Pouillet, S. Louveaux & M.V. Perez- Asinari, Data Protection and Privacy in Global networks : A European Approach, *EDI Law Review* 8, 147-196, 2001; P.M. Schwartz, European Data Protection Law and Restriction on International Data Flows, 80 *Iowa Law Rev.*, 1995, n°3, pp. 473 et s.; J.R. Reidenberg, E-commerce and Trans-Atlantic Privacy, 38, *Houston Law Rev.*, (2001), 3, pp.719 et ss..

⁵ Sur la notion de protection « adéquate » au sens de l'article 25.2 de la Directive, lire Y. Pouillet, B. Havelange avec la collaboration de M.H. Boulanger et A. Lefèbre, Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel, Rapport final du centre de recherches Informatique et droit élaboré pour la Commission européenne et publié sur le site du CRID (<http://www.crid.ac.be>)

⁶ A noter les décisions prises par la Commission à propos de différents systèmes législatifs jugés adéquats :
- Commission Decision 2000/519/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary – O.J. L 215/4 of 25.8.2000.
- Commission Decision 2000/518/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland-Official Journal L 215/1 of 25.8.2000.
- Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related frequently asked questions issued by the US Department of Commerce – Official Journal L 215/7 of 25.8.2000.
- Commission Decision 2002/2/EC of 20.12.2001 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act - O.J. L 2/13 of 4.1.2002.

autoréglementaires comme les « Safe Harbor Principles » proposés par le Department of Commerce des Etats Unis⁷ comme adéquats.

L'article 26 énonce quant à lui deux types d'exception à cette règle de la protection « adéquate », le premier type décliné en 7 cas par le point 1 de l'article vise des catégories de flux particuliers qui, en raison de leurs caractéristiques⁸, présente une légitimité et une proportionnalité telle que les risques d'atteinte sont limités voire réduits à néant. Le second point de l'article 26 prévoit que l'apport de « garanties suffisantes de protection des données » peut être opéré par d'autres modes de protection que ceux prévus à l'alinéa 1 : ce n'est plus l'environnement normatif externe au flux qui protège adéquatement les données mais bien la relation entre l'émetteur du flux et son destinataire. On songe bien évidemment au contrat⁹ que ces derniers pourraient conclure entre eux et dont les clauses « appropriées » auraient pour but et effet d'offrir des « garanties suffisantes », en d'autres termes une protection adéquate¹⁰. C'est dans ce contexte et sur cette base au vu des compétences que lui confie l'article 26.4, que la Commission avec l'aide du Groupe 29 a par deux fois émis des « clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers »¹¹. L'avis émis par le groupe dit de l'article 29 à propos des règles d'entreprise et dont nous discutons le bien-fondé s'inspire de la même philosophie. Les « garanties suffisantes » procèdent cette fois des règles d'entreprise contraignantes applicables au sein du groupe d'entreprises.

7. Sans doute, s'étonnera-t-on de cette nécessité d'ajouter encore aux options offertes aux entreprises localisées hors Europe pour échapper à l'interdiction de principe affirmée par

Cf. également à propos de la protection proposée par la loi récente d'Argentine, l'opinion du groupe dit de l'article 29 émis le 3 octobre 2002 (W.P. 63) disponible sur le site de la Commission européenne à l'adresse suivante : www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/

⁷ - Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/CE of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related frequently asked questions issued by the US Department of Commerce – Official Journal L 215/7 of 25.8.2000.

⁸ Sur la nécessité d'une interprétation restrictive des exceptions, lire B. Havelange et A.C. Lacoste, art.cité, p.246

⁹ Pour un commentaire sur l'apport de solutions contractuelles au problème de la protection des données, lire E. Longworth, Contractual Privacy Solutions, Towards Information Society and Electronic Citizenship, 22nd International Conference on Privacy and personal data Protection, Venezia, Sept. 2000, 183-203 ; J. Huet, Study on contracts involving the transfer of personal data between parties to Convention CoE 108 and third countries not providing an adequate level of protection, Council of Europe, Janvier 2001, disponible sur le site <http://www.legal.coe.int/dataprotection/> ,). Pour une analyse critique de ces clauses, lire B. Wellberry et R. Barcelo, European Commission's Model Contractual clauses : Paving the way for International Transfers or a New Hurdle, Privacy and Information Law report, Vol.1, 7, 2001, pp. 9 et s.

¹⁰ « La notion de « garanties suffisantes », au sens de l'article 26, paragraphe 2, renvoie à celle de « protection adéquate » (Groupe de l'article 29, Document de travail, n° 12, Transferts de données vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données, adopté par le Groupe le 24 juillet 1998, disponible sur le site de la Commission européenne : http://europa.eu.int/comm/internal_market/fr/dataprot/wpdocs/wp12fr.pdf

¹¹ Décision de la Commission 2001/497/CE du 15 juin 2001, J.O. L 181/19 du 4 juillet 2001 à propos des clauses contractuelles relatives à des transferts de données vers des responsables de données établis dans des pays tiers. Décision de la Commission 2002/16/CE du 27 décembre 2001, J.O. L 6/52 du 10 Janvier 2002 à propos des clauses contractuelles types pour le transfert de données vers des sous-traitants établis dans des pays tiers.

l'article 25. Sans doute, la souplesse européenne¹² démontrée par cette option supplémentaire la met un peu plus à l'abri si besoin en était, des critiques que les règles de l'OMC pourraient fonder¹³. En effet, il peut être difficile de ne pas reconnaître dans cette large palette de moyens laissés par l'application de la directive, une volonté de ne pas appliquer de barrières disproportionnées aux flux transfrontières : chaque entreprise peut trouver une solution appropriée à sa situation dont l'application ne représente pas un obstacle insurmontable.

L'ajout de l'option correspond en effet à cette volonté du groupe 29 de ne pas introduire de discrimination vis-à-vis des multinationales mal à l'aise vis-à-vis des autres options comme il est expliqué ci-après.

8. La « protection adéquate » nécessite la prise en considération des règles externes à l'entreprise, règles en vigueur et respectées dans le pays tiers. Sans doute, ces règles peuvent trouver leur origine dans des sources normatives diverses qu'elles soient de régulation publique ou privée (autorégulation professionnelle ou autres) voire de normes techniques de sécurité, qu'elles soient générales ou sectorielles mais elles doivent trouver une effectivité dans un territoire donné. La caractéristique des flux au sein d'une multinationale, dont les frontières géographiques sont définies de manière évolutive au rythme des acquisitions, des cessions et d'investissements nouveaux, interdit toute stabilité des règles applicables par la référence à un territoire, comme nous l'avons montré plus haut¹⁴.

Appliquer les exceptions de l'article 26.1. se heurtent également à la réalité de tels flux. Sans doute, le consentement indubitable et les nécessités de l'exécution d'un contrat conclu ou à conclure, hypothèses expressément prévues par l'article 26.1. peuvent justifier des transferts au sein de la multinationale. Ainsi, le membre du personnel peut-il consentir à ce que la donnée le concernant soit transférée vers le siège central où l'exécution du contrat passé avec lui peut-elle légitimer un tel transfert ? Ceci dit, il est difficile de trouver dans ces exceptions dont l'interprétation doit nécessairement être restrictive le fondement des solutions souples recherchées légitimement au sein des multinationales. Ainsi, la première exception prévue par l'article 26.1 réclame le consentement indubitable au transfert envisagé. Cette précision à la fois dans la modalité d'expression du consentement et dans le flux, objet de ce consentement ne rencontre pas les besoins d'un groupe qui souhaiterait comme nous l'avons montré pouvoir transférer les données d'un lieu à un autre, et envisager, selon les besoins du terrain, des transferts quantitativement et qualitativement variables.

9. Même objection à propos de l'utilisation de l'article 26.1.b) qui légitime le flux transfrontières de données uniquement lorsque ce flux, y compris son caractère international, est justifié de manière nécessaire, par les finalités contractuelles. Il est dès lors difficile pour une multinationale de plaider au regard de cette exception, la légitimité des transferts faits

¹² Sur ce refus de tout « impérialisme » européen dans les règles mises en place, Y. Poulet, « Pour une justification des articles 25 et 26 de la directive européenne en matière de protection des données à caractère personnel », *Liber Amicorum Bart de Schutter*, VUB Press, 2003, p. 243 et s.

¹³ A propos de l'application des règles de l' OMC au débat sur les règles européennes en matière de flux trans-frontières de données à caractère personnel, M.V. Perez-Asinari, « Is there any Room for Privacy and Data Protection within the WTO Rules? », *The Electronic Communications Law Review*, Kluwer, 2003; "The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-commerce Context?", 18th BILETA Conference:Controlling Information in the Online Environment, April, 2003, QMW, London, available at: <http://www.bileta.ac.uk/03papers/perez.html>

¹⁴ *Supra*, n° 5

dans l'intérêt d'une bonne gestion de la multinationale¹⁵. Ainsi, une banque de données centralisée hors Europe des employés de toutes les filiales, banque qui reprendrait la qualification des employés et leur historique au sein de la firme peut difficilement être qualifié de strictement nécessaire à l'exécution du contrat. Seuls des transferts ponctuels à partir des bases de données localisées sur un territoire national précis et relatifs à certains employés dont on recherche la mobilité pourrait répondre à cette double exigence de l'exception.

L'inadéquation des solutions contractuelles est tout aussi patente¹⁶. Sa mise en œuvre exige, c'est l'essence même de contrat, une parfaite identification non seulement des personnes contractantes mais des flux, objet du contrat. Or précisément, cette double nécessité apparaît difficilement satisfaite là où précisément le groupe d'entreprises entend jouer sur une multilatéralité des destinataires potentiels et l'extensibilité de l'objet des flux entre ces partenaires¹⁷.

Enfin, les trois options proposées jusqu'ici : la protection adéquate, les exceptions de l'article 26.1. et la solution contractuelle apportant des garanties suffisantes rencontrent toutes une limitation peu compatible avec les exigences des groupes multinationaux d'entreprises. Elles exigent que les territoires ou destinataires vers lesquels sont autorisés les transferts soient circonscrits et que soient évités les transferts « ultérieurs » (« onward transfers ») vers d'autres destinataires ou d'autres territoires non couverts par le contrat, l'exception de la protection adéquate. Comme nous l'avons dit (supra n° 4), le groupe d'entreprises est une réalité vivante qui ne peut exclure de tels transferts ultérieurs. Faudra-t-il chaque fois qu'un nouveau siège de la multinationale est créé et participe aux flux générés au sein du groupe, exiger tantôt la vérification de la protection adéquate y offerte (article 25.2), tantôt la signature d'un nouveau contrat (art. 26.2) avec le siège européen, tantôt le retour vers la personne concernée pour lui demander son consentement (art. 26.1).

10. De telles considérations, si elles justifient la création d'une option supplémentaire, ne doivent pas faire perdre de vue la nécessité d'assurer la continuité des principes de base mis en évidence dès 1998 dans le cadre des réflexions sur la protection adéquate et poursuivis dans la rédaction des clauses contractuelles types. Certes, le mode de réalisation de ces principes tient compte des spécificités de la réalité des groupes d'entreprise mais il s'agit toujours bien d'assurer une réelle et effective protection des données à caractère personnel. Il

¹⁵ On notera au passage que si l'article 26.1. reprend *mutatis mutandis* la plupart des fondements de légitimité des traitements prévus par l'article 7. Il omet soigneusement le seul qui eût pu être invoqué, à savoir celui de l'article 7f) qui permet de justifier le traitement lorsque l'intérêt légitime du responsable l'emporte sur ceux de la protection de la personne concernée (dans le même sens, les réflexions de Bellamy (Chief Privacy Officer de Accenture) reprises par M.V. Perez, How Accenture created a global approach to data transfers, Privacy Laws & Business International Newsletter, Sept. 2002, p. 9).

¹⁶ A ce propos, les réflexions de H.Rowe, Transfers of personal Data to third countries : the role of binding corporate rules, CL&SR, 19 , n°6, 2003, p. 491 et les réflexions tirées de l'expérience d'Accenture développées in M.V. Perez, How Accenture created a global approach to data transfers, Privacy Laws & Business Int. Newsletter, Sept. 2002, pp. 8 et ss. Il est à noter qu' Accenture avait dès 2001, avant même l'adoption par le Groupe dit de l'article 29, proposé une « Privacy policy » pour l'ensemble de son groupe et avait basé sa demande sur l'article 26.2. A l'époque, Accenture s'était vue refuser l'autorisation d'exportation des données.

¹⁷ "The code of practice approach taken by Accenture, said Bellamy (Chief Privacy Officer d' Accenture), can offer a truly seamless, practical and workable solution to suit the global nature of its business where functional boundaries have replaced national boundaries." (M.V. Perez, art. cité, note 16).

nous importerá dès lors dans le second chapitre de montrer tout à la fois, l'originalité et la continuité des solutions apportées.

II

La solution proposée : continuité et originalité

11. Le document de travail n° 12 : « Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données » constitue, parmi les documents produits par le groupe dit de l'article 29, la référence lorsqu'il s'agit de s'interroger sur la légalité des flux transfrontières.

Ce document est guidé par une approche fonctionnelle que par ailleurs nous avons caractérisée comme suit :

Cette approche repose sur une série de principes fondamentaux en matière de protection des données, ainsi que sur certaines conditions nécessaires pour garantir leur efficacité. En d'autres termes, deux types de règles sont censées garantir la protection adéquate, selon l'article 25.2 ou suffisante, selon l'article 26.2. Il s'agit des règles de fond relatives à la protection des données et de règles visant à assurer l'effectivité de ces règles dites de fond.

12. La première exigence à laquelle doit satisfaire l'autorégulation est de traduire de manière précise et détaillée les principes fondamentaux relatifs à la protection des données qui peuvent s'énoncer comme suit¹⁸ :

- limitation des transferts à une finalité spécifique ;
 - qualité et proportionnalité des données ;
 - transparence (des traitements) ;
 - sécurité ;
 - droits d'accès, de rectification et d'opposition ;
- restrictions aux transferts ultérieurs vers des personnes non couvertes par le champ d'application des règles de protection adéquate .

La façon dont l'exigence doit être appliquée en matière de groupes d'entreprises fera l'objet du premier chapitre. Nous analyserons ensuite la manière dont le Groupe dit de l'article 29 exige que ces principes soient effectivement respectés (Chapitre II)

Chapitre I : Les règles de fond et leur application en cas de groupe d'entreprises

13. Ce n'est pas sur ce point que le document de travail n° 74, « relatif à la protection des données aux règles d'entreprises contraignantes applicables aux transferts internationaux de données » se montre le plus innovant. Il se contente de les réaffirmer tout en prenant soin d'ajouter que ces principes fixant le contenu substantiel « doivent être développés et détaillés

¹⁸ Cette liste est reprise du document de travail n°12 (p. 5 et ss) et appliquée aussi bien à l'article 25.2 (protection adéquate qu' aux garanties suffisantes visées par l'article 26.2 (Cf. l'application aux contrats, p. 18). Aux éléments minima couverts par la liste reprise dans le texte, le document de travail n°12 ajoute d'autres principes qui peuvent exister dans des circonstances spéciales (données sensibles, système d'aide à la décision, etc.).

dans le cadre de règles d'entreprises contraignantes afin de pouvoir s'adapter de manière pratique et réaliste aux opérations de traitement effectués par l'organisation dans les pays tiers ».

L'ajout est important. Il se justifie, note le document de travail par le fait que l'absence de règles normatives externes explique que certaines entreprises membres du groupe situés dans des pays n'offrant aucune protection adéquate, n'ont dès lors aucune connaissance de la portée de principes comme ceux de la qualité et proportionnalité des données ou de la transparence. Ainsi, il n'est pas évident que les employés d'une filiale brésilienne puissent concevoir que le principe de transparence signifie une obligation d'informer les personnes concernées sur les finalités des traitements poursuivis et de s'interdire toute collecte de données par des méthodes déloyales. Détailler la signification pratique des divers principes a donc une valeur éducative et informative.

Le document de travail suggère une autre justification : la règle de la valeur ajoutée exigée des instruments d'autorégulation¹⁹ signifie que l'autorégulation est acceptable que dans la mesure où elle permet de préciser et compléter les principes généraux de la réglementation publique²⁰.

Au-delà de ces justifications explicite et implicite, on soulignera que cette exigence est parfaitement compréhensible. La norme dans la mesure où elle concerne des pratiques concrètes au sein d'un groupe d'entreprises se doit d'être plus détaillée que des normes externes qui doivent s'appliquer à de multiples situations²¹. On ajoutera que la valeur obligatoire des « règles d'entreprise » dépend bien évidemment de la précision de leur expression, comme il sera dit ci-après.

¹⁹ Sur la diversité des instruments d'autorégulation et une discussion de leur valeur, le lecteur se référera à l'ouvrage : « Gouvernance de la société de l'information », Cahier du CRID n°22, Bruylant-PUN, Bruxelles, 2002 (J. Berleur, C. Lazaro et R. Queck éd.). Cet ouvrage reprend des annexes et une bibliographie étendue sur le sujet.

²⁰ Ce principe de la valeur ajoutée est déjà sous-entendu par l'article 27 de la directive 95/46/CE qui encourage « l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions prises en application de la présente directive ». Au-delà on notera les réflexions sur la valeur de l'autorégulation menées par l'e-confiance online Forum mis en place le 30 mars 2000 par la DG SANCO et chargé de créer un consensus à propos de mécanismes capables de créer la confiance des consommateurs à propos des opérations de commerce électronique (travaux disponibles à l'adresse suivante : <http://dsa-isis.jrc.it/ECF/index.htm>). A propos de ce principe de l'« added value » lire nos réflexions in « les diverses techniques de réglementation de l'Internet : l'autorégulation et le rôle du droit étatique », Ubiquité, Juin 2000, p. 55 et ss.. Les instances européennes insistent dans plusieurs documents sur le fait que l'autorégulation doit compléter la réglementation des Etats membres, qui doit se contenter de fixer les standards sans entrer dans le détail. A cet égard, on notera le récent « Accord institutionnel « Mieux légiférer » », adopté par le Parlement européen le 8 octobre 2003 (disponible sur le site du parlement : <http://www3.europarl.eu.int/>) : « les trois institutions rappellent que la Communauté ne légifère que dans la mesure nécessaire, conformément au protocole sur l'application des principes de subsidiarité et de proportionnalité. Elles reconnaissent l'utilité de recourir...à des mécanismes de régulation alternatifs. La Commission veille à ce que le recours aux mécanismes de corégulation et d'autorégulation soit toujours conforme au droit communautaire et qu'il respecte des critères de transparence et de représentativité des parties impliquées. Ces mécanismes ne sont pas applicables si les droits fondamentaux ou des choix politiques importants sont en jeu.... » .

²¹ La même remarque vaut pour la solution contractuelle : la clause contractuelle type 2 « Détails du transfert » stipule : « Les détails du transfert, et en particulier les catégories de données à caractère personnel et les finalités pour lesquelles elles sont transférées, sont spécifiées ».

14. Une règle mérite une attention particulière : celle des « transferts ultérieurs ». La règle affirmée par le document de travail n° 12 selon laquelle « les transferts ultérieurs de données à caractère personnel effectués par le destinataire du transfert initial ne doivent être autorisés que lorsque le deuxième destinataire est également soumis à des règles offrant un niveau de protection adéquat », reçoit l'interprétation suivante :

- l'adjonction d'une nouvelle entité dans un groupe oblige le groupe, sous peine de voir les flux en direction de cette nouvelle entité considérés comme des transferts ultérieurs soumis à de sévères restrictions.

+ à s'assurer que cette nouvelle entité est effectivement liée par les règles du groupe et qu'elle est en mesure de les respecter,

+ à la tenue d'une liste de filiales mise à jour et la notification de modifications de cette liste une fois par an aux autorités de protection des données

- le flux vers une entité soit hors groupe soit membre du groupe, en cas de non respect des obligations mentionnées ci-avant, oblige à démontrer soit qu'une protection adéquate est offerte, soit la signature d'un contrat avec cette entité apportant une « garantie suffisante ».

15. L'avis n° 74 ajoute à ces réflexions que « les règles doivent clairement stipuler que lorsqu'une filiale du groupe a des raisons de penser que la législation qui lui est applicable risque de l'empêcher de remplir ses obligations en vertu des règles d'entreprise contraignantes et risque d'avoir un impact négatif sur les garanties fournies, ladite filiale en informera immédiatement le siège européen du groupe ». L'ajout est important et mérite une explication. Si la loi étrangère applicable à un membre du groupe oblige par exemple ce membre à écouter l'ensemble des communications ou à révéler les membres du personnel du groupe affilié à tel syndicat ou ayant telle ou telle croyance religieuse, cette législation étrangère oblige à un comportement qui pourrait contrevenir aux exigences de la protection adéquate requise par la directive européenne²².

Chapitre II : L'effectivité des règles

A. Rappel des règles

16. Trois conditions sont soulignées pour assurer l'effectivité des règles dont le contenu a été rappelé ci-avant :

- « assurer un niveau satisfaisant des règles ». On reconnaît, en général, ajoute le document de travail n° 12, la qualité d'un système à la conscience aiguë qu'ont les responsables du

²² ...à moins de pouvoir considérer que cette mesure est nécessaire au sein d'une société démocratique pour préserver des intérêts publics ou privés essentiels au sens de l'article 8 de la Convention européenne et repris par l'article 13.1 de la directive 95/46/CE, ainsi dans le cadre d'une lutte contre le terrorisme ou le blanchiment d'argent ou des raisons fiscales.

traitement de leurs obligations et les personnes concernées de leur droit. A cet impératif préalable de la connaissance des règles par les deux parties, s'ajoutent l'existence de mesures de contrôle internes ou externes de respect des règles et la consécration de sanctions efficaces et dissuasives.

- « apporter soutien et assistance aux personnes concernées ». Il s'agit d'abord du souci de protéger la partie faible : la personne concernée contre la partie forte, le responsable du traitement qui peut être le dispensateur de crédit, l'employeur dont on craint les foudres. Ce souci est comparable à celui qui inspire les législations de protection des consommateurs. Au-delà, l'exigence souligne la nécessité pour la personne concernée de pouvoir obtenir une aide face à la complexité et à l'opacité du fonctionnement des systèmes d'information.

Un accès rapide, efficace et non coûteux aux services appropriés du responsable des traitements et l'intervention d'une instance indépendante institutionnalisée et ayant compétence pour l'instruction des plaintes répond à cette seconde exigence.

- « fournir des voies de recours appropriées », suppose la possibilité, en cas de non respect des règles, d'une autorité indépendante publique ou privée compétente pour indemniser la victime ou sanctionner le contrevenant.

17. Dans quelle mesure, le document de travail n° 74 applique-t-il ces principes dans le cas particulier des multinationales ? La réponse à cette question nécessite une réflexion préalable. Dans la mesure où le caractère adéquat de la protection repose non sur des règles externes aux acteurs du flux mais sur des règles propres à ces acteurs, il importe de s'interroger sur le caractère contraignant de telles règles. La question mérite d'autant plus d'être posée qu'il n'est point fait recours au mécanisme du contrat dont chaque ordre juridique reconnaît la valeur obligatoire mais de simples règles générées par le groupe d'entreprise et auxquelles chaque membre du groupe déclare se soumettre.

On s'interroge donc sur la portée d'un règlement interne à une multinationale. Quelle valeur reconnaît à un document par lequel un groupe régule ses flux internes ? Le phénomène de l'autorégulation définie comme technique selon laquelle des règles de droit ou de comportement sont créés par les personnes auxquelles ces règles sont destinées à s'appliquer²³ est ici « unilatérale » dans la mesure où elle est le fait de celui qui prétend lui même la respecter et ne concerne que lui. A l'inverse des règles professionnelles ou de codes de conduite sectoriels, l'autorégulation n'est pas ici imposée de l'extérieur de l'entreprise ou à son groupe, elle est générée en leur sein sous forme d'une charte, d'un code de conduite d'une privacy policy du groupe ou d'un règlement édicté par la maison mère²⁴.

B. Le caractère contraignant des règles du groupe : Une double signification

²³ P. van Ommeslaghe, L'autorégulation : Rapport de synthèse, in L'autorégulation, Colloque Bruxelles 16 déc. 1992, Coll. Fac. Droit ULB, Bruxelles, Bruylant, p. 232. Cf. la définition donnée par P. Trudel, Les effets juridiques de l'autorégulation, 19 RDUS, 1988-89, n° 2, p. 251 et nos réflexions in Les diverses techniques de réglementation d'Internet, l'autorégulation et le rôle du droit étatique, Ubiquité, n° 5, juin 2000, p. 56 et s.

²⁴ Cf. à ce propos, la typologie « ratione personae » proposée par J. Berleur et T. Ewbank à propos des documents d'autorégulation in Gouvernance de l'Internet : Réglementation, autorégulation, corégulation ?, Gouvernance de la Société de l'Information, Cahier du CRID n° 20, Bruylant, Bruxelles, 2002, p. 34 et ss.

19. Pour le caractère contraignant de telles règles, le document de travail distingue le plan du droit (le caractère juridiquement exécutoire) et le plan pratique pour affirmer tout de suite que si le caractère contraignant doit être apprécié sur les deux plans, le second plan est important dans une configuration transfrontalière où la reconnaissance des droits s'avère difficile et où « il importe (dès lors) non seulement de veiller à ce que les règles internes soient exécutoires d'un point de vue juridique mais également d'un point de vue pratique ».

L'étude du CRID²⁵ à la base de l'adoption du document de travail n°12 : « Transfert de données à caractère personnel vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données » approuvé le 24 juillet 1998²⁶ plaide en effet pour une prise en considération, à côté des moyens fondés sur le droit et susceptibles d'entraîner condamnation judiciaire, de méthodes de contrainte fondées cette fois non sur le droit, mais la déontologie, la crainte de l'exclusion d'un secteur, ou de représailles médiatiques voire d'un boycott de l'entreprise.

L'existence de tels moyens contraignants d'essence non juridique prend dans le contexte d'un groupe une coloration particulière. Premièrement, ils sont aisés à définir et à mettre sur pied. Le document de travail n°74 que nous commentons note : « A cet égard, divers éléments s'avèrent pertinents, comme l'application de sanctions disciplinaires en cas d'infractions aux règles, une information personnalisée et efficace aux employés, la mise en place de formations spécialisées s'adressant aux employés et aux sous-traitants, etc.. ».

20. On sait que l'unité économique que peut représenter un groupe de sociétés ne se conçoit pas sans une structure hiérarchique forte et des moyens de contrôle importants du respect des décisions prises à la tête du groupe²⁷. La structure interne du groupe donne donc aux décisions d'autoréglementation prise en son sein et au plus haut niveau une force évidente mais, dans le même laps de temps, il faut bien reconnaître que dans le domaine qui est celui de la protection des données, l'intérêt poursuivi n'est pas nécessairement l'intérêt économique du groupe même si la bonne gestion des données nominatives peut contribuer à la bonne image du groupe. En d'autres termes, il n'est pas toujours évident que la règle, le code de conduite, la « privacy policy » décidée au sein du groupe fassent l'objet d'une attention particulière de la hiérarchie du groupe, s'il n'y a pas menace de contraintes cette fois juridiques, forçant la hiérarchie à utiliser les moyens de pression et de contrainte internes au groupe.

Deux autres facteurs atténuent fortement l'efficacité des moyens internes lorsque la multinationale est majoritairement implantée en dehors d'Europe. Le premier souligne la

²⁵ Y. Pouillet-B. Havelange, Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel, Jan. 97, Annexe au rapport annuel 1998 (XV D/5047/98) du groupe de travail établi par l'article 29 de la directive 95/46/CE, Office des publications européennes, ISBN 92-828-4305-X

²⁶ Ce document est accessible à l'adresse : <http://www.europa.eu.int/comm/privacy> .

²⁷ On pourrait difficilement accepter que les règles d'entreprise ne soient pas adoptées ou en tout cas explicitement avalisées par le sommet de la hiérarchie, par exemple par le Conseil d'administration de la maison mère du groupe. Quelle valeur pourrait être accordée à la déclaration d'un simple administrateur de filiale voire d'un président des implantations européennes du groupe, s'il n'y a pas d'une manière explicite une « couverture » de tels engagements par la maison mère.

difficulté pour la (ou les) filiale(s) européenne(s) minoritaire au sein du groupe de veiller au respect de règles pas nécessairement mais souvent proprement européennes. Le second constate que les règles internes motivées par les exigences européennes risquent de n'avoir pour champ d'application que les données à caractère personnel provenant d'Europe et d'introduire dès lors dans la gestion des flux et des bases de données une double réglementation : celle applicable à la majorité des données et dès lors mieux connue et celle plus exceptionnelle relative aux seules données européennes.

21. En conclusion, il est difficile de porter un jugement a priori et univoque à propos de l'efficacité des moyens de contraintes non juridiques. A priori, elle dépendra de la structure plus ou moins hiérarchisée du groupe de l'autorité au sein du groupe ayant adopté les règles, du poids des entreprises européennes dans le groupe et du champ d'application du règlement non restreint aux seules données « européennes ». On ajoutera que la création au sein de la multinationale d'un organe-relais indépendant²⁸, une sorte de « détaché à la protection des données », selon la terminologie de la directive 95/42, capable de veiller au respect des exigences légales représente une garantie complémentaire utile dans la mesure où ce « détaché » a une réelle compétence d'enquête et de contrôle, peut rapporter les défaillances constatées aux organes exécutifs centraux du groupe et proposer les corrections nécessaires.

On conçoit dès lors que le Groupe 29 ait exigé explicitement une nature contraignante des règles tant en droit qu'en pratique et souligner le caractère complémentaire de cette double contrainte même si le document souligne le caractère prépondérant de la contrainte non juridique « Si la possibilité pour les personnes concernées de faire respecter les règles en recourant à la justice constitue un élément nécessaire pour les raisons qui viennent d'être exposées, le groupe de travail « Article 29 » attache encore plus d'importance à l'application pratique de ces règles par le Groupe dans la mesure où il s'agit là de la finalité de toute approche fondée sur l'autorégulation²⁹. On ajoute que le document de travail n° 12 à propos de la protection adéquate n'opérait pas une telle distinction et ne se souciait pas dès lors d'affirmer cette complémentarité nécessaire.

22. S'agit-il donc d'une exigence nouvelle ? L'autorégulation externe pourrait-elle se contenter des seules mesures de contrainte non juridiques. Sans doute, l'adoption d'un code de conduite sectoriel contrôlé par des organes ad hoc, mis en place par le secteur et objet, en cas de non respect, de sanctions comme le boycott, la publicité par le secteur auquel appartient le contrevenant, voire l'exclusion du secteur pourrait conduire à prononcer une adéquation de l'autorégulation selon l'article 25.2. En matière de groupes d'entreprise, les mêmes mesures sont soit impensables, soit risquent de ne pas être mise en branle. Cette crainte d'une autorégulation, livrée à ses propres méthodes de contrôle et sanctions a déjà été relevée dans la discussion sur le caractère adéquat des « Safe Harbor » présenté par le Department of Commerce américain et considérés comme offrant une protection adéquate par décision de la Commission européenne le 26 juillet 2000³⁰. On sait que l'élément déterminant

²⁸ Le fait que le détaché soit un employé d'une société du groupe n'exclue pas l'indépendance de celui-ci. Tout dépendra de la compétence et du statut de ce détaché. Sa nomination a-t-elle été justifiée par sa compétence en matière de protection des données, un veto de l'autorité de protection des données compétente pour contrôler le respect des règles était-il possible ? Pouvait-il faire l'objet d'un licenciement pour fait de sa fonction ? Rapporte-t-il directement au Conseil d'administration de la maison mère ? etc..

²⁹ Document de travail n° 74, p. 12.

³⁰ Pour un commentaire très critique, lire J. Reidenberg, European Commission avoids Privacy disputes with the USA. », Privacy Laws and Bus. Int. Newsletter, Feb. 2002, p. 9 et ss.

du système proposé qui a finalement emporté la décision positive européenne a été la constatation que l'organisation (signatrice du Safe Harbor) est soumise aux pouvoirs légaux d'un organisme public³¹ « habilité à instruire les plaintes et à obtenir des mesures de redressement contre les pratiques déloyales ou frauduleuses ainsi que la réparation des préjudices subis par les personnes concernées, ... »³².

23. Le précédent du « Safe Harbor » mérite d'être relevé pour bien comprendre la difficulté de l'approche proposée ici. Dans le système du Safe Harbor, le caractère juridiquement contraignant du système d'autorégulation est indéniable mais indirecte : c'est dans la mesure où la loi américaine réprime les déclarations d'entreprises « deceptive or false » que la personne concernée, victime d'un non respect par l'entreprise de sa propre déclaration, pourra se plaindre auprès de cette « juridiction » particulière. Ce ne sont pas les règles elles-mêmes de protection des données qui sont ainsi protégées mais le fait de les avoir proclamées et de ne pas s'y tenir.

La nature juridiquement contraignante de règles d'entreprise proclamée unilatéralement³³ par un groupe d'entreprise est, en dehors de ce système propre aux Etats Unis, peu évidente. Comme le note Wéry³⁴, « la principale faiblesse de l'autorégulation unilatérale réside... dans son caractère unilatéral et donc en théorie non contraignant : créée par la volonté de celui qui accepte de s'y soumettre, la règle peut également être supprimée ou modifiée par déclaration unilatérale de volonté de cette même personne. ». Certes l'auteur se retranche finalement derrière la reconnaissance par le droit belge de l'acte unilatéral³⁵ pour rassurer le lecteur belge mais sa démonstration est un peu courte dans la mesure où il doit bien reconnaître que la solution même en Belgique est loin d'être pacifique et ne peut être facilement étendue à l'ensemble des droits européens³⁶.

³¹ En l'occurrence, la Federal Trade Commission (FTC). Sur le rôle essentiel de cette commission dans l'économie du système de protection prévue par le Safe Harbor, lire nos réflexions in « The Safe Harbor : An adequate Protection ? », Colloque international de l'IFCLA, Paris, Juin 2000, disponible sur le site du CRID (<http://www.crid.ac.be>) et celles de J.R. Reidenberg, E-Commerce and Trans-Atlantic Privacy, art. cité, pp.740 et ss. : « The agreement is predicated on the enforcement powers of Federal Trade Commission under section 5 of the Federal Trade Commission Act. »

³² Conformément aux dispositions de la Section 5 du « Federal Trade Commission Act » qui interdit les manœuvres et les pratiques déloyales ou frauduleuses dans le domaine du commerce ou de tout autre organisme remplissant une fonction analogue. Cf. la déclaration sur le site de la FTC (<http://www.ftc.gov/ftc/mission.htm>): FTC enforces a variety of federal and consumer protection laws and seeks to ensure that the nation's markets function competitively and are vigorous, efficient and free of undue restrictions. The Commission also works to enhance the smooth operation of the market place by eliminating acts or practices that are unfair or deceptive."

³³ Notre réflexion est différente à propos des codes de conduite ou auto réglementations multilatérales dans la mesure où il est aisé de voir dans de telles formes d'auto réglementation la définition d'usages propres aux secteurs ou de règles de l'art entraînant une responsabilité aquilienne des contrevenants au code.

³⁴ T. Verbiest, E. Wery avec la collaboration de A. Salaun et D. Gobert, Le droit de l'Internet et de la société de l'information, Larcier, 2001, p.526

³⁵ Cf. à ce propos la décision de la Cour de cassation belge du 21 janvier 1997 (Bull., 1997, V, n°31) où en l'espèce un employeur avait déclaré unilatéralement une augmentation de salaire et l'avait réduit par la suite.

³⁶ Ainsi, seule la loi allemande reconnaît légalement (§ 305 BGB) l'acte unilatéral mais exceptionnellement. L'exigence d'un contrat et la règle, qui ne subit de dérogation que dans la mesure où la loi en dispose autrement. Les auteurs français sont très réticents à une telle consécration (Cf. entre autres, J.L. Aubert, Encyclopédie Dalloz, Droit civil, 1987, v° Engagement unilatéral, n°9).

24. Sans doute n'est-il point nécessaire de passer par le détour d'une institution aussi controversée que l'acte juridique unilatéral pour affirmer la nature contraignante de règles, privacy policies ou autres déclarations (statements). Il doit être possible de considérer, selon le principe général de droit de la légitime confiance³⁷, que celui qui affirme sans détour un engagement public précis et circonstancié avec l'intention claire que cette volonté produise des effets de droit est tenu à l'égard des personnes vis à vis desquelles il a entendu s'engager. La constatation premièrement qu'in casu cet engagement est délivré à une autorité officielle comme l'autorité de protection des données chargée de veiller à la protection des personnes concernées, le fait que, deuxièmement, comme condition de l'autorisation d'exportation de données et troisièmement que cet engagement est l'objet d'une information de ces personnes bénéficiaires de l'engagement, plaident indiscutablement pour la reconnaissance d'une valeur juridique de ce type d'engagement. Le simple fait que l'engagement soit contenu dans un document intitulé « code de conduite » ou comme simples règles de comportement ne suffit pas en soi à exclure toute portée juridique au contenu précis et clair de l'engagement. La prépondérance du droit sur les autres ordres normatifs ou plutôt le fait que le droit puisse se mêler de donner efficacité à des prescrits moraux ou éthiques s'il l'estime juste et utile³⁸ conduit à présumer que le groupe qui proclame dans les conditions prévues par l'avis n° 74 une « privacy policy » est soumis au droit et que celui-ci donnera pleine efficacité à des engagements même pris sans référence explicite à la portée juridique de tels engagements³⁹.

Sans doute ce que nous affirmons ici devrait être l'objet d'analyses plus approfondies⁴⁰ et on peut concevoir l'extrême prudence du Groupe dit de l'article 29 lorsqu'il laisse aux groupes d'entreprises le soin de démontrer qu'au regard du droit déclaré applicable ces documents ont une réelle portée juridique⁴¹.

25. Cette première réflexion « sous réserve d'inventaire » conduit à reconnaître une portée contraignante aux règles visées par l'avis en question et ce vis à vis de leurs principaux

³⁷ A cet égard les réflexions éclairantes de M. Coipel, *La théorie de l'engagement par volonté unilatérale et son intérêt en particulier en droit des sociétés.*, in *Mélanges Van Ommeslaghe*, 2002, p. 21 et ss. L'auteur se réfère amplement à la thèse de Mr X. Dieux fondée sur le principe de confiance légitime.

³⁸ A cet égard, J. Ghestin, *Le juste et l'utile dans le contrat*, D.S., 1982, Chron., p. 1. F. Osman, *Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc : réflexions sur la dégradation des sources privées du droit*, R.T.D. civ., 1995, pp. 509 à 531.

³⁹ F. Osman, *Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc : réflexions sur la dégradation des sources privées du droit*, R.T.D. civ., 1995, pp. 509 à 531. M. Coipel, *Quelques réflexions sur le droit et ses rapports avec d'autres régulations de la vie sociale in Gouvernance de la société de l'information*, op. cit., p.61.

⁴⁰ En particulier, la question de la prise en considération de dommages non financiers du fait du non respect des règles n'est pas facile à résoudre. Elle constituait déjà dans le cadre des Safe Harbor un des points de discussion des plus délicats. Sur ce point, lire J.R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, art. cité, p. 745. L'auteur conclut: "For example, the memorandum presented by the U.S. Department of Commerce to the European Commission provides a lengthy discussion of the Privacy torts and indicates that the torts will be available. The memorandum failed to note that the applicability of these tort action shas never been established by U.S. courts and is, at present, purely theoretical..."

⁴¹ « But corporate groups must bear in mind that those applying for an authorization will have to demonstrate to the grantor of the authorisation that this is effectively the case throughout the group. » (Sur ce point et la difficulté de preuve, lire H.Rowe, art. cité, p.493).

bénéficiaires : les personnes concernées. En l'occurrence, ces tiers sont parfaitement déterminables dans la mesure où il est même fait devoir au groupe de les informer sur l'existence de ces règles. De ce fait, « ils doivent pouvoir faire respecter ces règles en introduisant une plainte aussi bien auprès de l'autorité compétente de protection des données qu'auprès du tribunal compétent... »⁴². Reste la question des entreprises qui au sein du groupe sont liées par cet engagement collectif pris par le groupe au nom des membres dont, en cas de non respect, la filiale européenne est responsable⁴³. A cet égard, l'avis commande la prudence : seules les entreprises directement contrôlées et soumises à l'unité de direction du groupe peuvent se sentir tenues du respect de ces règles à l'inverse de sociétés plus périphériques et autonomes⁴⁴. Vis à vis de ces dernières, l'avis recommande qu'un contrat avec stipulation pour autrui en faveur des personnes concernées soit conclu : « dans ce cas, la portée des droits liés au statut de tiers bénéficiaire correspondra au moins à celle prévue par la décision 2001/497/CE de la Commission relative aux clauses contractuelles types tant vis à vis de l'exportateur de données que de l'importateur de données⁴⁵ ». Ainsi, la Commission reconnaît clairement la complémentarité des deux types de garanties suffisantes imaginées sur base de l'article 26.2.

C. Analyse de l'application des trois conditions d'effectivité au cas de la multinationale⁴⁶

1. Assurer un niveau satisfaisant des règles

26. Cette première condition se décompose en différents sous-conditions : la « conscientisation » à la fois des destinataires des règles, les responsables de traitement et des

⁴² Avis, p.11.

⁴³ Sur la responsabilité de la filiale européenne, supra, n° 20

⁴⁴ A noter que l'avis précise que c'est au groupe à démontrer le caractère suffisamment étroit des liens pour que l'on puisse en déduire l'unité de direction et l'existence d'un rapport hiérarchique et de contrôle entre le centre de décision et les membres du groupe. On rappelle que la liste des membres du groupe soumis aux règles dites contraignantes doit par ailleurs faire l'objet d'une notification. On s'interroge sur la portée que ces explications pourraient avoir en dehors du contexte de la protection de la vie privée lorsque la responsabilité du centre de décision est mise en cause pour le fait d'un membre du groupe. Il est clair que dans un tel contexte, les plaideurs pourraient tirer argument de la déclaration faite auprès de l'autorité de protection des données pour inférer l'existence d'une responsabilité du groupe (sur cette responsabilité des groupes du fait d'une filiale sous son contrôle, lire C. Hannoun, op.cit., n°150 et ss. qui justifie cette responsabilité par la confiance légitime inspirée aux tiers du fait de l'existence de mécanismes internes de contrôle et de décision) ou pour appliquer certaines règles de compétence juridictionnelle, de protection des minorités, etc.

⁴⁵ Le texte de l'avis se réfère à la clause 3 qui prévoit que la personne concernée est tiers bénéficiaire des clauses contractuelles. Le mécanisme de la stipulation pour autrui pourrait expliquer dans nos droits continentaux cette exception à la relativité des contrats, principe également connu en droit anglo-saxon sous le concept de « privity of contracts ». On notera que le droit du tiers ne naît pas uniquement du contrat mais de la décision réglementaire de la commission prise en vertu des compétences qui lui sont conférées par l'article 26.4 de la directive. Ainsi, les personnes concernées pourront faire valoir leur droit nonobstant l'absence de validité du contrat auquel se rattache cette stipulation.

⁴⁶ Sur une application par une multinationale des conditions requises par le groupe de travail, lire le cas British Petroleum décrit par M. Kedde, How BP Makes its Global data Protection Policy a Working Reality ?, lors du colloque « Developing successful Privacy relationships » organisé par Privacy Laws and Business, 15th Annual conference, Cambridge, 1-3 juillet 2003.

bénéficiaires des règles, les personnes concernées est exigée mais en outre doivent exister des méthodes de contrôle internes ou externes du respect des règles. Finalement, des sanctions qualifiées « d'efficaces et dissuasives » doivent garantir le respect des règles dans la mesure où le responsable craindra les conséquences du non respect.

- La conscientisation des responsables, c'est-à-dire des différents unités du groupe et des personnes au sein de ceux-ci en charge des traitements suppose que le groupe demandeur du bénéfice de l'exception prévue à l'article 26(2) de la directive soit « à même de prouver que cette politique (de protection des données) est connue, comprise et effectivement appliquée ... » pour les employés, formés en conséquence⁴⁷ et disposant de toute l'information pertinente à tout moment, par exemple via l'intranet.

Porter à la connaissance des personnes concernées les règles d'entreprise est une exigence essentielle dans la mesure où cette information permettra le contrôle le plus effectif du respect des règles ; celui effectué par les personnes directement concernées par le traitement⁴⁸. L'avis du Groupe de l'Article 29 réaffirme le principe : « Les règles d'entreprise juridiquement exécutoires⁴⁹ doivent être portées à la connaissance des personnes et aisément accessibles par celles-ci »⁵⁰. En d'autres termes, outre les informations dont la fourniture est imposée par les articles 10 ou 11⁵¹ de la Directive 95/46 au responsable du traitement localisé en Europe, l'avis précise que la communication des données à d'autres filiales situées en Europe doit être l'objet d'une information spécifique et surtout que « les personnes ont facilement accès aux informations relatives aux principaux engagements pris par le groupe, les filiales liées par les règles ainsi qu'aux moyens mis à la disposition des personnes pour vérifier le respect des règles.

La formule laisse aux responsables le soin de déterminer la voie par laquelle cette information aura lieu. On le conçoit aisément : informer des employés d'une multinationale ne suivra sans doute pas les mêmes canaux qu'une information à donner à des internautes européens entrant via un portail localisé en Europe dans des sites multiples dont la gestion de la base de données clientèle est centralisée hors Europe.

- le contrôle du respect des règles peut être interne ou externe : « Les règles, affirme le groupe de l'article 29, doivent prévoir des audits internes et/ou externes réalisés régulièrement par

⁴⁷ L'avis souligne que les principes et concepts des réglementations européennes peuvent paraître obscurs pour des personnes situées en dehors de l'Europe et dès lors doivent être traduits en langage compréhensible par elles (Avis, p. 14).

⁴⁸ Dans le cas B.P., cité note 45, l'information vis à vis des employés appelés à appliquer les principes du code of practice est réalisée via un website « easy to use and jargon free –legal words- in order to describe data protection implications, designed for employees use and education ... The website has also a section dealing with news normally describing « risks » of non compliance... The tools section intends to encourage people to “ help themselves” “

⁴⁹ Pourquoi avoir limité aux règles juridiquement exécutoires. Ne faut-il pas sous réserve de secrets d'affaires, également informer à propos des mesures pratiques de contrainte ?

⁵⁰ Avis, p. 20.

⁵¹ L'article 10 vise les informations à fournir en cas de collecte auprès de la personne concernée ; l'article 11, celles à fournir lorsque la collecte a lieu auprès d'autres sources. Ces informations s'entendent tant de l'identité du responsable que des finalités du traitement. D'autres informations peuvent être exigées mais si cela est nécessaire pour assurer un traitement loyal des données.

des contrôleurs agréés qui transmettront un rapport directement au conseil d'administration de la maison mère du groupe »⁵², dont copie aux autorités de protection des données⁵³. L'avis va plus loin dans la mesure où il mentionne le devoir de coopération avec les autorités de protection des données qui peuvent exiger l'intervention d'experts ou intervenir eux-mêmes.

Nous reviendrons sur ce point à propos de la seconde condition d'effectivité.

- les sanctions en cas de non respect doivent être efficaces et dissuasives c'est-à-dire non purement correctives⁵⁴ L'avis est peu direct à ce propos si ce n'est sur un point. Le non respect du devoir de coopération avec les autorités de protection des données ou le non suivi de conseils donnés par ces autorités suite à un audit réalisé par ces dernières ou par des auditeurs internes ou externes et portés à la connaissance des autorités entraîne diverses mesures : la publication des conseils de l'autorité de protection voire la suppression ou le retrait de l'autorisation octroyée par l'autorité compétente en matière de flux transfrontières⁵⁵. Il est clair que d'autres sanctions internes au groupe pourraient être prévues. Sur base d'un rapport défavorable, les autorités responsables au sein du groupe, le Conseil d'Administration de la maison mère pourrait interdire la continuation de flux voire interdire le stockage de données chez certains membres du groupe. Des mesures disciplinaires pourraient être prononcées vis-à-vis des personnes en charge de traitements jugés non conformes aux règles d'entreprise. Le silence du groupe de l'article 29 sur de telles mesures pourrait se comprendre comme un certain scepticisme du groupe vis-à-vis de mesures dont le déclenchement est peu évident s'il contredit l'intérêt économique du groupe et si le poids de l'ancrage européen du groupe est peu significatif. Ce silence contraste avec l'intérêt que le Groupe dit de l'article 29 avait marqué dans son avis n° 12 à propos du « niveau satisfaisant de respect des règles » où étaient évoquées les sanctions disciplinaires, les mesures d'exclusion voire de boycott⁵⁶.

2. Fournir une assistance et une aide aux personnes concernées

27. Les groupes se doteront « d'un système de gestion des plaintes individuelles au sein d'un département clairement identifié ». Les personnes en charge de ce système jouiront d'un degré « approprié » d'indépendance. Tels sont les principes affirmés par l'avis mais on conçoit l'insuffisance de règles aussi minimales là où l'avis n° 12 affirmait⁵⁷ que : « Une exigence essentielle à laquelle doit répondre un système de protection des données approprié

⁵² Avis, p. 16. La note 15 ajoute que le contenu de ces contrôles sera exhaustif et décrira en détail certains points particuliers.

⁵³ Avis, p. 16. L'avis restreint cependant le devoir de remise d'une copie à deux cas ; copie automatique en cas de modification des règles notifiées, sur demande de l'autorité lorsqu'il y a coopération avec l'autorité.

⁵⁴ « Lorsqu'on examine les formes de sanctions existantes, il est important d'établir une distinction entre les sanctions « correctives » qui imposent simplement à un responsable du traitement des données, en cas de non respect du code, de modifier ses pratiques

⁵⁵ L'avis (p. 18) précise que ces décisions auront la forme d'un acte administratif pris par l'autorité compétente et seront notifiées à la Commission européenne voire publiées. Cette précision pose difficulté dans les pays où les autorités de protection des données n'ont pas compétence de décision comme en Belgique et ne pourraient dès lors être prise que par le Ministre compétent.

⁵⁶ Avis n° 12, p. 13.

⁵⁷ Avis n° 12, p. 14

et efficace est qu'une personne physique confrontée à un problème touchant aux données personnelles la concernant ne soit pas laissée à elle-même mais puisse bénéficier d'un soutien institutionnel pour la solution de ses problèmes. » et surtout « mettait en garde contre des instances appartenant à la profession ou au secteur concerné, considérées comme insuffisamment neutre dans la mesure où ces instances partagent des intérêts communs avec le responsable mis en cause. »⁵⁸. A fortiori, aura-t-on quelque difficulté à considérer qu'un département du groupe même autonome dans sa gestion pourrait être neutre vis-à-vis des intérêts du groupe dont il relève. On conçoit dès lors que l'assistance et l'aide doivent provenir de l'extérieur du groupe ?

L'avis n° 74 répond à cette inquiétude dans la mesure où il désigne cette instance externe neutre : l'autorité de protection des données dont relève le membre du groupe sis dans l'Union européenne. La solution étonne par sa radicalité dans la mesure où elle écarte toute solution « autoréglementaire », ainsi on aurait pu imaginer que l'assistance soit le fait de sociétés ou d'associations de libertés choisies par le groupe à la limite sur une liste agréée par le Groupe dit de l'article 29. Ce refus de considérer d'autres solutions peut s'expliquer par la crainte à la fois des responsables de traitement de se trouver confrontés à des associations peu contrôlées et contrôlables ayant peu le souci du secret professionnel en particulier mais également des autorités de protection des données peut confiantes dans l'efficacité du soutien qui pourraient apporter ces instances aux personnes concernées, de leur absence de moyens réels d'investigation et finalement au manque de moyens de sanctions en leur possession. On note, autre requis de l'avis n° 12, que l'accès aux autorités de protection des données est sans doute plus aisé que vis-à-vis d'autorités privées peu connues, souvent situées en terre étrangère et peu au courant des règles européennes.

28. Si ces explications convainquent, on ne peut que noter que les solutions ici retenues ne reprennent pas la solution des « Alternative Dispute Resolution Mechanisms » pronées par les « Safe Harbor Principles », et dont l'action est décrite en particulier par le F.A.Q. n° 11⁵⁹. On souligne que selon les Safe Harbor Principles, la coopération avec les autorités de protection des données était mise sur le même pied que la désignation de ces « ADR ». Quelques doutes avaient été émis à propos de cette équivalence et de « l'effectivité du support de ces ADR aux personnes concernées ». Ainsi, nous concluons⁶⁰ : « L'exigence européenne prévue par le groupe dit de l'article 29 de trouver auprès de cet organisme « support and assistance » n'est pas reprise. Certes, l'accès doit être, selon les Safe Harbor, « aisé » et « à un coût raisonnable » mais ne fallait-il pas prévoir –surtout vis à vis d'une personne située en pays lointain- que l'organisme puisse investiguer d'initiative sur simple plainte et non être comme le conçoit le système américain, uniquement un lieu de résolution des litiges, ce qui exige que la personne concernée développe elle-même ses griefs et arguments... Enfin des doutes peuvent être élevées sur l'effectivité de certaines sanctions. Que se passe t'il si l'organisme incriminé refuse de modifier ses pratiques ou de dédommager les victimes de ses agissements ?...

⁵⁸ Avis n° 12, p. 14.

⁵⁹ Les Safe Harbor Principles, ainsi que les Frequent Asked Questions (FAQ) et la liste des entreprises ayant souscrits aux principes (+ ou – 400 entreprises) sont publiés sur le site : <http://www.export.gov/safeharbor.htm>

⁶⁰ Y. Pouillet, Les Safe Harbor : une protection adéquate ?, texte présenté lors du colloque de l'IFCLA , Paris 15-16 juin 2000, Paris , déjà cité ; J. Reidenberg, E-Commerce and Trans-Atlantic Privacy, 38 Houston Law Rev.,2001, pp.740 et ss. ; L. Costes, ..., Lamy Droit de l'informatique, cahier n° , 2000, p....

29. Faut-il voir, dans la suppression du choix entre deux modes d'assurer le soutien : celui offert par les ADR et celui né du recours auprès des autorités européennes de protection des données, un recul de l'autoréglementation ou une méfiance vis-à-vis de celle-ci⁶¹. Il est clair que si la solution peut apparaître rassurante en théorie, du moins aux défenseurs de la vie privée, la pratique risque de révéler rapidement l'absence de moyens des autorités de protection des données d'accomplir la tâche de support et d'assistance aux personnes concernées. Quoi qu'il en soit des « Safe Harbor » à l'avis n° 74, il semble bien que le Groupe dit de l'article 29 fasse jouer un rôle de plus en plus essentiel aux autorités de protection des données.

c) offrir des voies de recours appropriées :

30. La condition traitée ici renvoie bien évidemment à l'analyse déjà faite du caractère contraignant des règles et du droit des personnes concernées à se prévaloir de ces règles. Il importe qu'une voie de recours existe pour ces dernières qui lui permette non seulement la correction des opérations passées et non conformes aux règles mais également une indemnisation des dommages et financiers et moraux (ce que le système juridique anglo saxon qualifie de « distress ») des conséquences de ce non respect.

L'avis n° 74⁶² énonce en ce sens que « les règles stipuleront que les personnes concernées bénéficieront des droits en matière de réparation et de responsabilité visés aux articles 22 et 23 de la directive⁶³ dans les mêmes conditions et dans la même mesure que si le traitement effectué relevait du champ d'application de la directive relative à la protection des données... ». L'avis ajoute quelques précisions qui alourdissent le caractère contraignant de la règle : le siège européen ou la filiale européenne responsable par délégation de la protection des données « devraient » accepter d'une part d'endosser la responsabilité⁶⁴ et de prendre les mesures nécessaires pour réparer les actes commis par les autres filiales du groupe hors

⁶¹ Dans les clauses contractuelles types, la clause 8 mentionne comme suit « la coopération avec les autorités de contrôle » : « Les parties conviennent de déposer une copie du présent contrat auprès de l'autorité de contrôle si un tel dépôt est prévu par le droit national ». La clause 7 prévoit en cas de litige avec la personne concernée, cette dernière puisse choisir de soumettre le litige soit à la médiation d'une personne indépendante ou, le cas échéant, à l'autorité de contrôle », soit aux tribunaux du for de l'exportateur. La clause 5 d) prévoit, si d'autres solutions ne sont pas possibles, qu'à la demande de l'exportateur, un audit puisse être réalisé par l'exportateur ou un organe de contrôle composé de membres indépendants ... choisi par l'exportateur et, le cas échéant avec l'accord de l'autorité compétente. Enfin, l'importateur selon la clause 5 c) coopérera avec l'autorité de contrôle compétente lors de demandes de renseignements de cette dernière et se rangera à l'avis de cette même autorité en ce qui concerne le traitement de données transférées.

⁶² Avis, p.18

⁶³ Pour rappel, l'article 22 prévoit que la personne concernée dispose d'un recours juridictionnel et l'article 23 facilite l'obtention de dommage par la personne concernée en prévoyant un renversement de la charge de la preuve. Sur cette disposition peu claire, entre autres commentaires, lire T. Léonard- Y. Pouillet, La protection des données à caractère personnel en pleine (r)évolution, J.T., 1999, p. 394.

La clause 6.1 des clauses contractuelles types reprises en annexe de la décision de la Commission du 15 juin 2001 déjà citée affirmait dans le même sens que « Les parties conviennent qu'elles ne pourront être exonérées de cette responsabilité que si elles prouvent que l'action incompatible avec les obligations prévues par les présentes clauses n'est imputables à aucune d'entre elles. »

⁶⁴ L'avis précise même que la filiale européenne doit démontrer qu'elle a les ressources financières suffisantes pour assumer cette responsabilité ou qu'une assurance en responsabilité civile couvre ce genre d'incidents.

Europe et d'autre part d'être poursuivie judiciairement dans l'Union européenne⁶⁵. Cette solution de la responsabilité conjointe de l'établissement européen et de l'établissement hors Europe fautif avait déjà été imposée dans le cadre des clauses contractuelles types : « L'exportateur et l'importateur de données conviennent d'être solidairement responsables des dommages subis par les personnes concernées résultant d'une violation (des obligations contractuelles). » Il s'agit là comme ici de faciliter le recours⁶⁶ de la personne concernée en mettant à charge de l'établissement européen la responsabilité de l'ensemble des agissements du groupe. A lui, de démontrer que la violation incriminée n'est pas le fait d'un membre du groupe. On ajoute que le groupe par ces règles doit reconnaître le droit des personnes concernées d'intenter une action contre le groupe et ce devant la juridiction soit de l'établissement européen à l'origine du transfert, soit de l'établissement responsable de la protection des données.

31. On s'étonnera à nouveau de la manière dont le Groupe dit de l'article 29 restreint les choix des multinationales quant au choix de l'instance en charge de résoudre les litiges. L'avis n°12, de même que les décisions sur les contrats types, n'exclut pas bien au contraire l'intervention d'arbitres voire d'organes de médiation et on sait combien les « Safe Harbor Principles » avaient fait usage de cette liberté en prévoyant simplement l'obligation pour les sociétés américaines qui désiraient bénéficier des avantages de la protection adéquate de choisir un organe de régulation des litiges privé, un A.D.R.. Les clauses contractuelles types allaient dans le même sens : l'importateur pouvait convenir qu'en cas de litige, soit une médiation conduite par une personne indépendante ou par l'autorité de protection des données serait menée, soit le tribunal de l'exportateur européen serait saisi, soit enfin un arbitrage serait conclu. Comment expliquer cette restriction voulue par le groupe dit de l'article 29 à propos des modes de résolution des litiges en cas de flux à l'intérieur d'une multinationale si ce n'est par une crainte que les autres modes de résolution ne soient pas à suffisance effectifs dans la mesure où pèsent de lourdes incertitudes sur le caractère contraignant au plan juridique des règles émises et que la multinationale puissante⁶⁷ ne choisisse un mode de résolution devant un ADR peu au courant du contenu et surtout de la signification des règles de protection des données ?

⁶⁵ L'avis va jusqu'à préciser le renversement de la charge de la preuve, stipulé par l'article 23 de la Directive : au cas où un dommage survient dû, suivant les dires de la personne concernée au non respect des règles du groupe, c'est à la filiale européenne à démontrer que le dommage n'est pas imputable à un membre du groupe. Une preuve qui pour la personne concernée « serait impossible à matérialiser et qui de toute façon supposerait des efforts et un investissement en temps et en argent disproportionnés de la part de la personne concernée » (avis, p . 19).

⁵⁹ Le recours contre l'importateur doit rester « exceptionnel » selon les décisions relatives aux clauses modèles types du 15 juin et du 27 décembre 2001 « lorsque cela se révèle approprié... dans les cas où l'exportateur de données a matériellement disparu ou a cessé d'exister en droit ou est devenu insolvable ». on peut supposer que la même règle s'applique mutatis mutandis à l'hypothèse des groupes de sociétés.

⁶⁷ N'oublions pas qu'en matière de contrat d'exportation de données, il y a négociation entre l'importateur et l'exportateur qui craint que sa responsabilité ne soit engagée. On peut supposer que les deux forces sont dès lors plus en équilibre dans le modèle contractuel que lorsque la personne concernée se retrouve face à une multinationale puissante qui décide unilatéralement du contenu de ces « règles » et des modalités de leur application. En ce qui concerne cette fois le Safe Harbor, le libre choix laissé à l'entreprise américaine à propos des modes de résolution des litiges peut se justifier par le fait que ce libre choix n'exclue pas la possibilité de saisir la très officielle Federal Trade Commission qui peut statuer chaque fois que la privacy policy émise par l'entreprise et se référant aux principes du Safe Harbor « constitue un « false or deceptive statement » (A propos de cette Commission aux compétences juridictionnelles, lire nos réflexions in Y. Pouillet, Les Safe Harbor Principles : une protection adéquate ? , art. cité.

CONCLUSION

32. L'avis n° 74 complète la panoplie des modes d'obtention de la « protection adéquate », requise par la directive pour assurer dans un contexte international la protection des données à caractère personnel.

Le fait-il adéquatement ?

Premièrement, il est patent que les autres modes de protection dits adéquats répondaient mal aux spécificités des flux existant à l'intérieur d'un groupe d'entreprises.

Deuxièmement, l'avis ne s'écarte pas d'un certain nombre d'acquis des réflexions menées jusqu'ici : ainsi l'avis n° 74 se situe dans la droite ligne des réflexions menées depuis 1998 à propos de la protection adéquate. Les exigences relatives tant au contenu des règles à adopter par la multinationale qu'à leur effectivité sont directement déduites de l'avis n° 12 relative au concept de protection adéquate et les clauses contractuelles types décidées par la Commission sur base de l'article 26.4 ont inspiré outre le souci que les règles d'entreprise créent un droit vis-à-vis des personnes concernées, la nécessité d'une responsabilité de l'entité européenne, membre du groupe.

Troisièmement, l'avis est l'occasion de mettre en évidence la différence entre une autorégulation multilatérale ou sectorielle et celle unilatérale que se fixe un groupe. Sans doute, cette différence justifie-t-elle le malaise ressenti par les auteurs de l'avis vis-à-vis de l'effectivité des règles dites d'entreprise. Indiscutablement, plus d'une association sectorielle, la multinationale jouit de moyens de contraindre pratiquement ses membres à respecter les règles qu'elle fixe : la forte hiérarchie et les structures de contrôle qui caractérisent le groupe d'entreprises garantissent en effet ce respect. Encore faut-il que la multinationale entende utiliser ces moyens ! A juste titre, l'avis considère indispensable de doubler les moyens de contrainte juridique y compris à disposition des personnes concernées et offrant des recours juridictionnels en Europe ; l'avis donne un rôle important aux autorités européennes de protection des données, seuls support et assistance crédibles des personnes concernées ; enfin, l'avis impose une lourde responsabilité aux membres européens du groupe ou tout au moins à l'un d'entre eux.

Cette prudence, si elle est louable, est-elle « adéquate » ? Les autorités de protection des données se retrouvent en première ligne pour assurer la protection des données alors même qu'elles sont débordées et singulièrement mal armées pour faire face à des multinationales puissantes.

Quant à ceux qui voient dans l'avis n° 74 une victoire supplémentaire de l'autorégulation, une analyse un peu sérieuse de l'économie de l'avis témoigne au contraire des limites d'une autorégulation certes plus souple, plus précise dans son contenu, plus imaginative dans ses modes de contrôle et des sanctions mais, dans le même temps, cette autorégulation ne voit ses qualités s'épanouir, que dans la mesure à la crainte du recours au juge et de l'intervention du gendarme officiel qu'est la Commission. Bref, l'autorégulation fait place à la co-régulation définie comme un « effective mix »⁶⁸ d'intervention à la fois des pouvoirs publics et privés ;

⁶⁸ selon l'expression de l'OCDE. Cf également la définition donnée par le récent accord institutionnel européen déjà cité : « On entend par corégulation le mécanisme par lequel un acte législatif communautaire confère la

la complémentarité des moyens mis par l'un et l'autre de ces pouvoirs visant à assurer une meilleure effectivité du principe consacré par la règle légale, en l'occurrence l'exigence de protection adéquate.

réalisation des objectifs définis par l'autorité législative aux parties concernées reconnues dans le domaine (notamment les opérateurs économiques, les partenaires sociaux, les organisations non gouvernementales ou les associations). Sur ce « concept », lire parmi d'autres, l'ouvrage : « Gouvernance de la société de l'information », Berleur et alii, Cahier du Crid n° 22, Bruylant, 2002.