La protection des données à caractère personnel en droit communautaire

Boulanger, Marie-Helene; Moreau, Damien; Léonard, Thierry; Louveaux, Sophie; Poullet, Yves; de Terwangne , Cécile

Published in:
Journal des Tribunaux. Droit Européen

Publication date:
1997

Document Version
le PDF de l'éditeur

pas destinataires qui sont visés dans ces «situations exceptionnelles», alors pourquoi ne pas les mentionner? En réalité, force est de constater qu'il ne s'agit pas ici d'une décision, mais d'un refus d'adopter une décision. Dès lors, peut-on étendre la jurisprudence *Plaumann* à ce type d'hypothèse? Cette question, ainsi que la deuxième, est donc tributaire de la réponse donnée à celle relative à la nature du refus de la Commission d'adopter une décision.

Ce refus peut-il être considéré comme un véritable acte à l'encontre duquel un recours en annulation ou un recours en carence pourrait être intenté? À suivre les conclusions de l'avocat général sur ce point, la réponse paraît positive, du moins en ce qui concerne un recours en annulation. En effet, M. La Pergola conteste la jurisprudence antérieure du Tribunal, au sens où celle-ci a assimilé, selon lui de manière inexacte, la procédure de manquement et la procédure de l'article 90, § 3. Certes, la confusion vient du fait que les deux procédures sont déclaratives d'une violation par l'État d'une obligation découlant du traité. Mais, non seulement «la place et la finalité de l'article 90 plaident en ce sens que le particulier ne saurait, en l'espèce, être privé de la protection juridictionnelle dont il bénéficie dans le domaine essentiel de la concurrence», mais de plus, «il est clair que la disposition en question ne peut pas être valablement assimilée à l'article 169 [...] destiné à régir les rapports institutionnels sur le plan communautaire»[41]. La Cour semble avoir été sensible à cet argument, ce qui clarifie sans aucun doute les relations entre les articles 169 et 90, § 3, du traité[42]. Dès lors, un particulier démontrant son intérêt individuel et direct à ce qu'une décision de la Commission au titre de l'article 90, § 3, du traité soit adoptée pourra faire valoir cet intérêt en introduisant un recours en annulation du refus de prendre une décision, ce refus étant assimilé à une décision négative[43]. Cette décision de rejet étant à rapprocher d'un rejet définitif d'une plainte dans le cadre de la mise en œuvre de la procédure des articles 85 et 86, ou d'une position définitive de la Commission relative à la qualification d'une aide d'État[44], seules susceptibles de faire l'objet d'un recours en annulation[45]. Mais en tout état de cause, l'arrêt de la Cour aurait gagné en clarté si cette dernière s'était expressément prononcée en faveur de l'assimilation entre «décision négative» et «refus d'adopter une décision», à l'instar de son avocat général, dont elle confirme cependant, selon nous, implicitement le raisonnement.

Pour ce qui concerne le recours en carence, la situation semble plus claire, pour autant qu'on en déduise que le refus de la Commission constitue un acte. Dans cette hypothèse, la carence ne peut être alléguée puisque le refus lui-même constitue la preuve de l'action de la Commission. Cela permet dès lors d'écarter la thèse, précédemment défendue par le Tribunal, selon laquelle le seul véritable motif de l'irrecevabilité d'un recours en carence était le pouvoir discrétionnaire de la Commission, tout en ménageant ce même pouvoir en consacrant l'irrecevabilité d'un recours en carence. À ce titre, la solution paraît satisfaisante.

Par contre, il semble que la Cour entende implicitement permettre un recours en carence des particuliers à l'encontre d'un refus de la part de la Commission de *se prononcer sur une plainte*. En effet, le recours de la Bilanzbuchhalter n'est écarté que parce qu'il visait à obtenir une décision de condamnation de la législation allemande, et non parce que la Commission ne s'était pas prononcée sur sa plainte[46]. Dans cette dernière hypothèse, il semble que la Cour serait prête à admettre un recours en carence, après que le particulier eut mis la Commission en demeure de se prononcer, conformément à l'article 175 du traité. Si une telle interprétation revient à consacrer des garanties procédurales semblables à celles accordées aux particuliers dans la mise en œuvre des articles 85 et 86 du traité, l'on peut d'ores et déjà parier que cet arrêt entraînera un contentieux intéressant à suivre, que ce soit dans le cadre de l'article 90, § 3, du traité ou de son extension à la protection des droits des plaignants en matière d'aide d'État.

Meri RANTALA
DEEA, Collège d'Europe, Bruges, Promotion Alexis de Tocqueville

Vincent KRONENBERGER
DEA droit communautaire, Université des sciences sociales de Toulouse, doctorant en droit communautaire

(41) Conclusions précitées, point 17.
(42) Pour plus de détails sur la comparaison entre ces deux procédures, v. F. MELIN-SOUCRAMANIEN, *op. cit.*, p. 601.
(43) Conclusions de M. LA PERGOLA, *op. cit.*, points 14 et 20.
(44) T.P.I., arrêt du 22 mai 1996, *AITEC*, aff. T-277/94, *Rec.*, II-351, points 51-52.
(45) V. en ce sens, B. GOLDMAN, A. LYON-CAEN et L. VOGEL, *Droit commercial européen*, 1994, p. 558.
(46) Notons que ceci peut se concilier avec la jurisprudence dans le domaine des aides d'État, dans laquelle le Tribunal de première instance a seulement écarté un recours en carence des particuliers visant à ce que la Commission prenne position dans un sens déterminé et non qu'elle se prononce sur leur plainte: cf. T.P.I, arrêt *AITEC*, précité, point 66.

Dossier

LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN DROIT COMMUNAUTAIRE

Troisième partie*

B. – Les flux transfrontières vers des pays tiers

a. – Le principe: la nécessité d'une protection adéquate[152]

72. – 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[153] 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 transferts» 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 d'autres concernent 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.

73. – Le texte de l'article 25 suggère une triple approche de la notion de «protection adéquate»:

– *une approche au cas par cas*[154], c'est-à-dire que la situation de la protection des données dans un pays tiers est évaluée «par rapport à un transfert déterminé ou une catégorie de transferts»;

– *une approche souple et ouverte* puisque selon le libellé même de l'article 25, 2, l'évaluation doit pouvoir tenir compte à la fois des

* Les deux premières parties de cet article sont parues dans nos précédentes livraisons: *J.T.D.E.*, 1997, pp. 121-127 et pp. 145-155.
(152) Sur l'étude de cette notion, voy. Y. POULLET, B. HAVELANGE (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 européenne, février 1997, à paraître.
(153) Le texte ne précise pas de qui relèvera l'appréciation du caractère adéquat ni quel rôle l'autorité de contrôle jouera dans cette procédure.
(154) Par opposition à une approche législative qui se fonderait sur la seule comparaison des textes en vigueur dans le pays tiers par rapport à la directive.

particularités propres 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 en application de 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 telle qu'organisée par la directive. En effet, la notion de protection adéquate induit la confrontation des exigences de protection de la directive avec les réponses données par les pays tiers. Il s'agit de rechercher s'il y a «similarité fonctionnelle». La «similarité fonctionnelle» implique que l'on recherche non la transposition pure et simple des principes et systèmes de protection européens dans le 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 législative complète[155].

74. – Quelques éclaircissements s'imposent encore au sujet de la notion d'«adéquation».

Tout d'abord, cette notion suppose un référent permettant 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. Sans doute faut-il considérer qu'il s'agit des principes de base de la directive, sans s'arrêter à la forme ou aux modalités particulières attachées à ces principes dans le texte européen.

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[156]. 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 ne précise pas ce qui serait une durée acceptable ou non. De même, le texte communautaire ne détaille pas ce que devrait être le «contenu minimum» d'une législation ou encore ses conditions d'application, pour considérer qu'elle assure un niveau adéquat de protection[157].

Enfin, à propos des instruments de protection mis en place dans le pays tiers, l'article 25 se réfère non seulement aux normes issues de l'autorité publique, qu'elles soient générales ou sectorielles[158], mais également aux codes de conduite[159] voire aux mesures techniques, pourvu que ces instruments soient «respectés». Ainsi, la personne chargée d'évaluer la protection étrangère sera plus attentive à l'«effectivité» d'un instrument qu'à sa nature: ce qui importe, c'est que la connaissance de l'instrument, même s'il s'agit d'une simple *company privacy policy*, soit largement répandue parmi les personnes concernées et les responsables des fichiers; de même, on sera attentif à la possibilité d'un recours des particuliers à l'encontre des responsables de fichiers en cas de non-respect des instruments en question.

75. – L'article 25, alinéas 1 et 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 démarche est évidemment lourde pour les États membres, aussi les articles 25, 4, et 25, 6, ouvrent deux voies d'allégement de la tâche par le biais de la Commission. 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[160].

76. – En ce qui concerne les bénéficiaires de la protection adéquate, la directive se limite à protéger les données des personnes bénéficiant au départ de la protection de la directive lorsque ces données sont envoyées à l'étranger.

Par conséquent, ce que la directive impose, ce n'est pas une protection s'appliquant à l'ensemble de la population mondiale, mais plutôt la garantie aux personnes bénéficiant au départ de la protection de la directive, du maintien d'une protection adéquate pour les traitements même non soumis à la directive. Ainsi, le responsable étranger d'un traitement pourrait, sans modifier les règles de protection qu'il suit habituellement, réserver aux seules personnes originairement bénéficiaires de la protection européenne, la «protection adéquate» de l'article 25.

b. – Les exceptions

77. – La directive édicte certaines exceptions au principe de l'article 25, «sous réserve de dispositions contraires du droit national régissant des cas particuliers»[161]. De la sorte, des transferts de données à caractère personnel vers des pays n'offrant pas un niveau de protection adéquat peuvent avoir lieu en certaines circonstances. Deux types d'exception sont prévus: le premier tient compte du contexte dans lequel s'inscrit le flux; le second substitue un mode de protection *ad hoc*, à la protection adéquate: le contrat.

À propos de la première catégorie d'exceptions, l'article 26, 1, *a*, vise l'hypothèse où la personne concernée a indubitablement donné son consentement à l'opération de transfert. On ne peut parler de véritable consentement que si celui-ci est «éclairé»[162], c'est-à-dire si la

(155) La notion de protection équivalente est utilisée par la Convention n° 108 du Conseil de l'Europe en son article 12. Cet article met à charge d'une partie contractante une obligation de permettre les flux de données sensibles vers les autres États parties à la Convention qui assurent une protection équivalente à celle de l'État émetteur. 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, voy. 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», *D.I.T.*, 1991/2, p. 58 et s.

(156) L'article 25, 2, énonce qu'il faut «en particulier» prendre en considération tel ou tel élément.

(157) À cet égard, l'article 25, § 6, dispose qu'un pays tiers peut être considéré comme assurant un niveau de protection adéquat «en raison de ses engagements internationaux». La question se pose de savoir s'il faut considérer sur base de cette disposition qu'un État tiers, partie contractante à la Convention n° 108, offre un niveau de protection adéquat. Une réponse positive signifie qu'en présence de flux transfrontières la directive n'offre pas un niveau de protection plus élevé que la Convention n° 108. En cas de réponse négative, les États membres de l'Union qui sont également parties à la Convention peuvent être pris dans une situation inextricable. En vertu de la directive, ils ne pourront autoriser certains flux, alors qu'en vertu de l'article 12, 2, de la Convention n° 108, ils ne pourront les empêcher (sauf concernant certaines données sensibles). À ce jour, seuls trois États sont parties contractantes à la Convention sans être membres de l'Union: la Slovénie, la Norvège, l'Islande.

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

(159) 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 la possibilité de recours. 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.

(160) Analyse au cas par cas et analyse globale: les deux types d'analyse 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 conduisent de façon évidente à la reconnaissance de l'adéquation ou l'inadéquation de la protection offerte.

(161) «Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit 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

ersonne concernée a conscience qu'il s'agit ien d'un flux transfrontalier, si elle connaît le ays de destination des informations qu'elle ransmet et réalise que ce pays n'assure pas un iveau de protection adéquat des données. D'autres exceptions existent. Elles concernent les transferts nécessaires 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[163]. Sont également visés les transferts servant à la sauvegarde d'un intérêt vital ou d'intérêts publics importants, ou encore s'opérant dans le cadre d'une action en justice. L'article 26, 1, *f*, prévoit encore le cas des transferts à partir d'un registre public «destiné réglementairement à l'information au public et ouvert à la consultation» (ainsi, par exemple, le registre du commerce).

On notera qu'il importe que le transfert soit nécessaire au regard de tels intérêts et qu'il ne suffit pas que l'intérêt contractuel existe pour que le transfert soit autorisé[164]. Ainsi, dans le cadre d'une multinationale, la création en terre lointaine d'une banque de données relative à l'ensemble des travailleurs et les flux engendrés à partir des filiales européennes ne pourront bénéficier de l'exception de l'article 26 que si le responsable démontre qu'il existe une nécessité d'opérer ces transferts pour l'exécution du contrat.

La seconde catégorie d'exceptions vise des substituts fonctionnels à la protection adéquate élaborée par la directive. Les clauses contractuelles sont visées en particulier[165]. 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 les traitements. À propos de ce second type d'exception, une autorisation de l'État membre est nécessaire[166]. L'accorder revient à reconnaître le caractère «suffisant» des garanties offertes. L'État membre doit informer la Commission de telles autorisations, des oppositions pouvant être exprimées par d'autres États membres. On souligne à ce propos, le rôle important joué par la Commission qui peut, après délibération des représentants des États membres[167], inviter[168] les États membres à agir: soit à accepter de telles mesures palliatives, soit à les rejeter ou proposer des mesures supplémentaires.

C. – L'applicabilité extraterritoriale de la directive

78. – Selon l'article 4, 1, *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[169].

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 couvrirait les hypothèses où la collecte des informations, opérée par exemple en Belgique, est suivie d'un transfert des données vers l'étranger pour les y traiter à meilleur prix. Correspondrait aussi à recourir à des moyens situés en territoire communautaire le fait d'interroger depuis l'extérieur de l'Union une banque de données sise en Belgique. L'applicabilité de la directive s'étendrait même à un système de réservation aérienne dans la mesure où c'est en interrogeant une boîte aux lettres tenue à sa disposition en Europe par une agence de voyages, que la personne désireuse d'opérer une réservation prend connaissance de messages EDI qui lui sont destinés.

Bref, l'interprétation large de la notion de «recours» aboutirait à décréter que la quasi-totalité des flux transfrontières amènerait le destinataire des flux à tomber sous le coup des dispositions de la directive. Point ne serait besoin alors des articles 25 et 26 de la directive, puisqu'en toute hypothèse cette dernière serait applicable.

Lors d'une analyse récente de l'application de la directive à Internet, une autre interprétation, qualifiée de «téléologique», du critère de rattachement défini par l'article 4, 1, *c*, a été proposée[170]. L'argumentation sous-tendant cette interprétation s'articule comme suit:

«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 États 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 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. Une protection adéquate des données envoyées à l'étranger en provenance de l'Union est exigée.

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 retenue 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 E. MONTERO (éd.), *Internet face au droit*, Cahier du CRID n° 12, Bruxelles, Story-Scientia, 1997, p. 211). À côté de cette interprétation large, la notion de «cas particulier» pourrait toutefois s'envisager comme laissant la possibilité pour l'autorité nationale de n'intervenir que pour un flux déterminé et de ne déroger qu'exceptionnellement et non par catégorie aux différentes hypothèses prévues par l'article 26.

(162) Sur cette notion, cf. *supra*.

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

(164) L'article 26 constituant une exception doit s'interpréter de manière stricte.

(165) Des mesures techniques *ad hoc* pourraient également être envisagées. Sur les contrats comme moyen supplétif d'assurer une protection équivalente ou adéquate dans les flux transfrontières, voy. C.M. PITRAT, «Clauses modèles pour les flux transfrontières de données ou comment assurer une protection équivalente», *D.I.T.*, 1993/1, pp. 46 à 52; L. EARLY, «Securing equivalent protection among nations in the context of TBDF: a possible role for contract law», *D.I.T.*, 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, la Commission européenne et la CCI (Strasbourg, 2 nov. 92, T.PD[92] 7 revised). À noter que la recommandation R (89)2 sur la protection des données utilisées à des fins d'emploi envisage explicitement la possibilité de recourir au contrat pour garantir que le destinataire sis dans un pays tiers respecte les principes énoncés dans la recommandation (cf. Exposé des motifs, paragraphe 63).

(166) Pour une critique judicieuse de ce modèle, lire l'article de J. REIDENBERG, «Setting Standards for Fair Information in the US. Private Sector», *Iowa Law Review*, March 1995, Volume 80/n° 3.

(167) Il est à noter que dans ce cas, le groupe d'experts (reprenant des membres des autorités de protection nationales) ne joue pas de rôle explicite... La matière, on le pressent, est hautement politique.

(168) Cette invitation devra, pour devenir décision, suivre la procédure de comitologie définie par la décision du Conseil du 13 juillet 1987, fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission, *J.O.C.E.*, 1987, n° L197/34.

(169) Comp. avec l'obligation imposée par l'article 1, § 6, de la loi belge à charge du maître du fichier situé à l'étranger de nommer un représentant auprès duquel les droits d'accès et de rectification s'exerceront. La même idée est poursuivie par la directive.

(170) C. DE TERWANGNE, S. LOUVEAUX, *op. cit.*, p. 237 et s. et M-H. BOULANGER, C. DE TERWANGNE, «Internet et le respect de la vie privée», *op. cit.*, p. 202. Les auteurs se réfèrent également à la lecture du considérant 20 de la directive et à l'exposé des motifs de la première proposition de directive émanant du Conseil (proposition du 15 oct. 1992, COM(92) 422 final – SYN 287, p. 13).

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.

– celle où le flux est le fait exclusif d'un responsable localisé dans un pays tiers. Il en est ainsi d'un logiciel qui permettrait à un responsable sis à l'étranger de visiter 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.

En conclusion, l'article 4, 1, *c*, viserait des hypothèses exceptionnelles soit celle où la localisation du responsable est anormale au regard de son activité orientée vers l'Union européenne et portant sur 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 le 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 de transfert de données, d'un responsable de traitement situé dans le territoire de l'Union européenne.»

VI. – LES CODES DE CONDUITE

79. – La directive prévoit que les États membres et la Commission «encouragent» l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales[171]. Les rédacteurs de tels codes pourront les soumettre aux autorités de contrôle qui en vérifieront la conformité au regard de la réglementation[172].

Le texte envisage également l'élaboration de codes communautaires qui peuvent, quant à eux, être soumis au groupe européen de protection des données[173] qui examinera notamment s'ils respectent les dispositions nationales[174].

Lorsque des codes seront soumis à leur approbation, tant l'autorité nationale de contrôle que le groupe européen pourront recueillir, «s'ils l'estiment opportun», les observations des personnes concernées ou de leurs représentants. En outre, selon qu'il s'agira d'un code national ou communautaire, chacune de ces deux instances pourra respectivement en assurer la publicité.

80. – L'adoption de codes de conduite en aval des réglementations nationales issues de la directive peut se révéler très positive lors de la mise en œuvre des normes protectrices. Émanant des secteurs eux-mêmes, ces codes sont en principe élaborés au niveau le plus approprié – celui où surgissent les problèmes – et sont dès lors en mesure d'énoncer des solutions adaptées aux réalités, traduisant de manière concrète les principes formulés en termes généraux dans les réglementations[175]. Au surplus, ils sont aisément modifiables, ce qui leur permet de suivre facilement les évolutions des secteurs. Un argument de type économique – censé jouer sur l'image du responsable du traitement – peut encore être relevé: les codes de conduite, pourraient, selon certains, améliorer la confiance de la personne concernée dans les services proposés par une entreprise qui s'y soumet volontairement. On soulignera enfin l'intérêt des codes communautaires qui devraient contribuer à réduire pour un même secteur les divergences entre les protections mises en place au sein de chaque État membre.

On ne peut toutefois passer sous silence certains de leurs inconvénients. Largement issus d'une démarche volontaire, la sanction de leur non-respect peut être difficile à mettre en œuvre[176]. À la limite, leur adoption peut servir d'alibi pour offrir une façade de respectabilité aux organismes concernés. Certes, rien n'empêche les États de leur reconnaître une valeur réglementaire ou de prévoir des procédures d'homologation officielle. Toutefois, cette démarche se heurte souvent au problème de la représentativité des instances à la base des codes.

Les codes ne sont pas non plus soumis à une publicité organisée et ne tiennent compte que dans une certaine mesure de l'intérêt des personnes concernées. En effet, même si leurs rédacteurs sont souvent conscients de la nécessité d'assurer une protection de ces dernières, ils la transposent dans leur logique propre, généralement sans que n'existe de réel débat permettant d'assurer une juste mise en balance des intérêts en présence.

Par ailleurs, l'élaboration de ces codes de conduite n'est pas chose aisée dans la mesure où traduire les dispositions à caractère général des réglementations de protection des données en mesures spécifiques, peut donner lieu à des interprétations divergentes. On doit cependant relever que pareille démarche constitue souvent l'occasion d'une prise de conscience des enjeux de la protection des données de même que l'occasion de nouer un dialogue productif entre les milieux professionnels et les autorités de contrôle.

En tout état de cause, les codes de bonne conduite n'exemptent pas les secteurs de l'application des législations nationales issues de la directive qui garantiront, en termes généraux certes, le respect des droits subjectifs et les possibilités de recours des personnes concernées[177]. Cette soumission à la loi, en définitive, apporte aux codes sectoriels, ne fût-ce qu'indirectement, une effectivité certaine étant donné que la loi s'accompagne de force juridique contraignante qui reste l'ultime garantie de l'efficacité des principes énoncés.

VII. – LES ORGANES DE CONTRÔLE

A. – Le contrôle au niveau national

81. – Confirmant l'approche retenue dans les législations nationales issues de la Convention du Conseil de l'Europe[178], la directive impose à chaque État membre d'instituer en son sein une ou plusieurs autorités publiques, chargées de surveiller l'application des réglementations édictées. Elle énonce, en outre, les grands principes régissant la mise en place de ce type d'autorités, mais laisse toutefois aux États membres la liberté de décider de l'op-

(171) Article 27, § 1, de la directive. À noter que le paragraphe 39 du Rapport explicatif de la Convention n° 108 insiste également sur l'intérêt de mesures réglementaires volontaires, tels des «codes de bonne pratique ou des règles de conduite». La recommandation R (85) 20 du Conseil de l'Europe relative aux données utilisées à des fins de marketing (précitée) va dans le même sens.
(172) Article 27, § 2, de la directive. Par les mots «peuvent être soumis», la directive prévoit la possibilité de consulter l'autorité de contrôle, mais ne l'impose pas.
(173) Cf. *infra*.
(174) Cf. *infra*, le groupe institué par l'article 29 de la directive. L'examen au regard des dispositions nationales adoptées en application de la directive pourrait donner lieu à quelque difficultés dans la mesures où ces législations peuvent présenter des divergences significatives (cfr. supra). Quelle sera dès lors la référence en matière de codes communautaires?
(175) À moins, bien sûr, qu'il ne s'agisse d'un simple «recopiage» de ces principes.
(176) Il existe de multiples variétés de codes de conduite. Le degré d'effectivité de chacun de ceux-ci s'évaluera en fonction de circonstances propres à leur adoption et à leur mise en œuvre. On notera, à titre d'exemple, le pouvoir des organismes ou fédérations sectorielles vis-à-vis de leurs membres, l'existence de mécanismes de suivi, la portée concrète de leurs dispositions ou encore la publicité qui leur est donnée.
(177) De manière similaire, le paragraphe 39 du Rapport explicatif de la Convention n° 108 ne les envisage qu'en tant que complément utile à des mesures de type contraignant (lois, règlements, directives administratives, etc.) et insiste sur le fait que de telles mesures «ne suffisent pas par elles-mêmes pour donner suite à la Convention».
(178) À titre d'exemple, en France, la Commission nationale de l'informatique et des libertés (CNIL), en Belgique, la Commission de la protection de la vie privée, en Allemagne, le délégué fédéral à la protection des données élu par le Bundestag et compétent pour les traitements des organismes publics fédéraux et pour le secteur privé, et par ailleurs des autorités de contrôle désignées par les Länder, et aux Pays-Bas, la Registratiekamer. À noter que la Convention n° 108 ne prévoit pas l'institution d'autorités de contrôle, mais bien celle d'autorités destinées à favoriser la coopération entre les États signataires. Par contre, la recommandations R (87) 15 relative aux données de police (précitée) suggère explicitement la mise en place d'autorités de contrôle.

portunité d'en établir une ou plusieurs[179] et d'en déterminer exactement la «physionomie».

Les autorités de contrôle sont supposées exercer en toute indépendance les missions dont elles sont investie[180]. Il s'agit là d'une de leurs caractéristiques fondamentales censée permettre qu'émergent des solutions équilibrées tenant compte des divers intérêts en présence. Cette caractéristique se reflétera, par exemple, dans le fait que les autorités ne sont pas intégrées dans une hiérarchie administrative classique, qu'elles jouissent d'une autonomie budgétaire, que leurs membres ne peuvent être relevés de leurs fonctions, que des mesures d'incompatibilité frappant ceux-ci sont édictées, que leur composition garantit une pluralité d'opinions et assure une certaine représentativité des personnes concernées. En pratique, l'indépendance peut pourtant se révéler une véritable gageure. En effet, d'un côté, la composition des autorités révèle souvent l'empreinte des pouvoirs politiques en place, ce qui peut freiner la mission protectrice des organes lorsque des mesures contestables sont adoptées par les gouvernants[181], et de l'autre côté, certaines autorités peuvent être tentées de défendre d'une manière paraissant excessive les droits et libertés des individus, mettant de la sorte en jeu leur crédibilité.

82. – La directive entérine les approches nationales en termes de missions et de pouvoirs dévolus aux autorités de contrôle. De manière générale, ces dernières seront chargées de la surveillance de l'application de la réglementation. Pratiquement, on peut, pour l'essentiel, mettre en évidence trois formes d'interventions. Premièrement, elles ont un rôle de conseil à l'égard du pouvoir réglementaire. La directive n'impose cependant pas que les avis émis soient conformes[182]. Deuxièmement, les autorités tendent à «éveiller les consciences», non seulement en informant le public de la portée des droits et obligations résultant de la législation, mais également en assurant une certaine publicité aux prises de position portant sur des questions particulières[183]. Troisièmement, elles interviennent en tant qu'arbitre dans les conflits entre ficheurs et fichés, permettant de dégager des solutions qui, tout en intégrant les prescrits légaux, ménagent les intérêts légitimes des uns et des autres. On se doit de préciser que la saisine des autorités de contrôle peut être effectuée par toute personne ou association la représentant[184] et que les décisions «faisant grief» sont susceptibles de recours juridictionnel.

83. – Pour que les autorités de contrôle puissent remplir leurs missions de manière efficace, la directive impose de leur reconnaître des pouvoirs d'investigation. Définis en termes larges, ces pouvoirs ont pour objet de permettre aux autorités d'accéder aux données traitées et de recueillir toutes informations nécessaires à leur tâche[185]. En outre, des possibilités spécifiques d'intervention doivent leur être octroyées, telles l'émission d'avis préalablement à la mise en œuvre des traitements[186], la publication appropriée de ces avis, la possibilité soit d'ordonner le verrouillage, l'effacement ou la destruction de données, soit d'interdire un traitement (à titre définitif ou temporaire) ou d'adresser un avertissement ou une admonestation au responsable du traitement, soit enfin de saisir les parlementaires nationaux ou d'autres institutions politiques.

La directive reconnaît aux autorités le pouvoir d'ester en justice ou de porter les violations constatées à la connaissance du pouvoir judiciaire. Jusqu'à présent, les États membres privilégiaient fréquemment la deuxième solution[187]. Les deux possibilités sont à présent explicitement prévues.

84. – On doit encore signaler que lorsque des dispositions nationales sont adoptées en application de l'article 13 de la directive[188], chaque autorité de contrôle peut être saisie par toute personne d'une demande de vérification de la licéité d'un traitement. Si cette procédure s'apparente en partie à ce que certains pays, comme la Belgique et la France, ont mis en place pour des traitements particuliers, chargeant l'autorité de contrôle de l'exercice du droit d'accès[189], elle s'étend plus largement à un examen général de la licéité des traitements pour lesquels des mesures législatives ont limité la portée de certaines obligations.

Par ailleurs, les autorités de contrôle sont tenues de publier un rapport d'activité. On insistera sur l'importance de la publication de tels rapports. C'est en effet par cette voie que les organes rendent compte de l'accomplissement de leurs missions devant les parlements qui les ont institués, mais surtout, cette transparence permet aux acteurs de la vie économique et politique d'avoir connaissance des positions des autorités de contrôle et d'adapter leur comportement en conséquence.

La directive prévoit également que les autorités de contrôle coopèrent entre elles[190]. En termes d'expertise développée par chacune d'entre elles, cette collaboration relève du bon sens dans la mesure où les réglementations nationales trouveront un fondement commun dans la directive et dès lors qu'il est indispensable d'éviter que les responsables de traitement ne soient tentés de faire usage de manière abusive de la liberté des flux de données à caractère personnel reconnue par la directive. En outre, dans la mesure où les problèmes se posent fréquemment de manière similaire dans chacun des États membres, autant bénéficier de l'expérience de l'étranger...

85. – En définitive, l'impact des autorités de contrôle au sein des États membres qui les instituent, dépendra de leurs réelles possibilités d'action, à savoir le fait de disposer d'incitants ou de sanctions suffisamment forts pour que leurs prises de position soient suivies d'effets. L'impact de l'action de ces autorités est également étroitement lié à la qualité de leurs décisions et au fait que ces dernières sont adoptées en connaissance de cause, et plus particulièrement sur la base de discussions approfondies avec les intéressés. On peut cependant s'interroger sur l'effectivité de leurs moyens d'intervention face à des délocalisations de traitements dans des lieux non soumis à leur compétence et en présence de technologies de traitement de l'information évoluant sans cesse[191].

(179) Les États membres sont libres d'opter pour une seule autorité chargée de l'ensemble des questions de protection des données ou pour plusieurs autorités exerçant leurs activités dans des domaines spécifiques. On doit souligner que la deuxième solution implique la mise en œuvre de procédures efficaces permettant aux diverses autorités d'agir de manière concertée.

(180) Le 62e considérant qualifie l'institution d'autorités de contrôle exerçant leurs fonctions en toute indépendance d'élément «essentiel» pour la protection des personnes.

(181) De manière paradoxale, lorsque l'État décide de la mise en place d'importants traitements de données à caractère personnel, l'intervention d'autorités de contrôle peut conduire à renforcer le pouvoir de celui-ci, lorsque celles-ci avalisent son intervention, garantissant par leur «indépendance» que la protection des droits et libertés des citoyens est suffisamment prise en compte.

(182) La directive ne prévoit pas explicitement que les avis revêtent un caractère obligatoire. La formulation de article 28, § 2, de la directive envisage la consultation des autorités de contrôle «lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel». Tout dépendra donc de l'appréciation des instances réglementaires quant à l'impact des mesures envisagées sur la protection des droits et libertés des personnes.

(183) L'obligation d'établir un rapport d'activité participe clairement à cette mission d'information du public (cf. *infra*). D'autres moyens peuvent cependant être envisagés, comme les communiqués de presse, les brochures d'information, etc.

(184) En vertu de l'article 28, § 4, la personne concernée doit être informée des suites réservées à sa demande.

(185) Les législations en vigueur dans les États membres accordent généralement de tels pouvoirs aux autorités actuellement en place. On peut citer à titre d'exemple, la loi française du 6 janvier 1978 qui reconnaît, en ses articles 11 et 21, à la Commission nationale de l'informatique et des libertés le pouvoir de se faire communiquer tous renseignements et documents utiles à sa mission, mais exclut tout pouvoir contraignant tel que perquisition ou saisie. La Convention n° 108 ne prévoit, quant à elle, rien de comparable.

(186) Cf. *supra*, la notification. Voy. à titre de comparaison, l'article 1.3 de la recommandation R(87) 15 sur les données de police (précitée) qui suggère que l'avis de l'autorité de contrôle soit recueilli préalablement à la mise en œuvre d'un traitement automatisé.

(187) Il en est ainsi pour la loi française de 1978 qui ne reconnaît à la CNIL que le pouvoir de dénoncer une infraction au parquet qui, quant à lui, reste libre de classer ou non l'affaire.

(188) Cf. *supra*.

(189) Cette procédure est connue en France sous le vocable d'«accès indirect». Elle concerne par exemple l'accès aux traitements liés à la sécurité de l'État, aux services de renseignements, à la police.

(190) De la même manière, l'article 13, *a*, de la Convention n° 108 prévoit une collaboration entre autorités, par la fourniture d'informations tant sur les réglementations et pratiques que sur des éléments de fait concernant les traitements de données effectués sur leur territoire.

(191) À l'origine, l'instauration d'autorités de contrôle répondait précisément au besoin d'apporter des réponses rapides, éclairées et adaptées à des problèmes que les pouvoirs traditionnels semblaient peu à même d'appréhender. Dans ce contexte, la recherche d'une médiation faisait figure d'approche privilégiée.

B. – Le contrôle au niveau communautaire

a. – Le groupe européen de protection

86. – La directive instaure, en son article 29, un groupe européen de protection des personnes à l'égard du traitement des données à caractère personnel[192].

Divers groupes à vocation internationale s'occupaient déjà de questions de protection des données. Ainsi, la Convention du Conseil de l'Europe avait institué un comité consultatif chargé d'améliorer la Convention, de l'interpréter ou de la réviser[193]. Par ailleurs, la conférence des commissaires européens avait spontanément vu le jour à l'initiative des autorités de contrôle européennes existantes, en réaction précisément au projet de directive[194].

87. – Le groupe institué par la directive est dénué de pouvoir décisionnel. Il est composé d'un représentant de l'autorité ou des autorités de contrôle nationales désigné par chaque État membre, mais comprend, en outre, un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et un représentant de la Commission européenne[195].

Il a pour mission de contribuer à la mise en œuvre homogène des lois nationales, de donner un avis à la Commission sur le niveau de protection dans la Communauté et les pays tiers[196], de conseiller la Commission pour amender la directive et de donner un avis sur les codes de conduite communautaires. Le groupe peut également émettre des recommandations sur toute question concernant la protection des personnes et établit un rapport annuel publié[197].

88. – La reconnaissance par la directive de l'intérêt de prévoir un forum de discussions entre commissaires européens est une démarche positive. Il est en effet important de donner une portée concrète à l'article 28, § 6, et d'institutionnaliser la coopération entre les autorités de contrôle. Mais ne devrait-on pas franchir une étape supplémentaire et octroyer à ce groupe des pouvoirs effectifs d'intervention?

Par ailleurs, hors la directive et le droit communautaire, différents textes règlent l'échange de données à caractère personnel dans le contexte du troisième pilier du traité de Maastricht[198] et ont institué en matière policière, douanière et judiciaire, chacune pour la matière qui la concerne, une autorité de contrôle (autorité de contrôle commune Europol, autorité de contrôle Eurodac, autorité de contrôle commune S.I.D.). Le paradoxe de cette situation provient de ce que chacune des instances n'est compétente que pour les données visées par la convention qui l'institue. Or, les services utilisateurs font usage de l'ensemble des données rendues disponibles par les différentes conventions. En outre, on peut craindre que les autorités sectorielles enfoncées dans leurs problèmes spécifiques, ne perdent de vue les questions plus générales et la nécessité d'une approche globale de celles-ci. À terme, ne serait-il pas dès lors préférable qu'une seule et même autorité soit chargée de contrôler l'ensemble des données échangées dans le cadre du troisième pilier du traité de Maastricht?

b. – Le contrôle au niveau des institutions communautaires

89. – Il serait utile que soit instaurée une autorité de contrôle chargée de veiller au respect des règles de protection des données par les institutions communautaires. Une résolution du Parlement européen a été adoptée en ce sens[199]. La directive n'étant pas applicable aux autorités européennes, celles-ci ne sont pas tenues de mettre en place une telle instance[200]. Sa mise en place nous paraît cependant fondamentale en vue de garantir la protection des données à caractère personnel lors des échanges d'informations entre les États membres et les institutions communautaires. Le projet de traité d'Amsterdam, adopté lors du Conseil européen des 16 et 17 juin 1997, prévoit d'ailleurs de combler ces lacunes par l'insertion d'un nouvel article 213B dans le traité instituant la communauté européenne. En vertu de cette disposition, la directive sera applicable aux institution communautaires à partir du 1er janvier 1999, tandis qu'un organe indépendant de contrôle aura été institué avant cette date, comme, bien entendu, que le traité d'Amsterdam entre en vigueur.

c. – L'exécution des mesures communautaires

90. – Enfin, l'article 31 institue un groupe composé des représentants des États membres et présidé par le représentant de la Commission. Son rôle consiste à assister la Commission dans l'exécution de la directive, en particulier en ce qui concerne le transfert de données vers les pays tiers[201]. La composition de ce groupe, à savoir les représentants des États membres, indique à suffisance l'enjeu éminemment politique de cette question. Ce groupe peut dans une certaine mesure être comparé au comité d'experts du Conseil de l'Europe qui élabore les recommandations. Toutefois, son pouvoir semble s'apparenter davantage à celui d'un organe consultatif selon la procédure fixée par la comitologie[202].

VIII. – RECOURS, RESPONSABILITÉS ET SANCTIONS

91. – Deux types de recours sont prévus en cas de violation des lois nationales prises en conformité avec la directive.

L'article 22 prévoit la possibilité pour les États membres d'organiser un recours administratif devant les autorités de contrôle et cela, préalablement à la saisine de l'autorité judiciaire.

Les États membres ont cependant l'obligation d'offrir à la personne concernée par les données un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question.

La nature du recours et ses règles propres tombent pour le reste dans la compétence souveraine des États membres.

92. – L'article 23 proclame, dans la suite de l'existence du recours, le droit de la personne concernée d'obtenir du responsable du traitement réparation des dommages subis du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la directive. Le second alinéa de cette disposition permet aux États membres d'exonérer le responsable du traitement s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Ce texte pourrait donner lieu à des difficultés d'interprétation. Il n'est en effet pas aisé de déterminer s'il introduit un système de responsabilité classique fondé sur la preuve d'une faute, d'un dommage et du lien causal ou si cette responsabilité est présumée de la simple constatation du dommage naissant d'un traitement illicite ou d'une action incompatible avec les règles nationales. L'absence de référence à la notion de faute – un traitement illicite et, *a fortiori*, une action «incompatible» avec les dispositions nationales n'impliquent pas forcément une faute dans le chef du responsable du traitement[203] –, la

(192) Ce groupe qui se réunit au rythme de quatre réunions par an, fonctionne de manière effective depuis le mois de janvier 1996.
(193) Articles 14, 19 et 20 de la Convention n° 108.
(194) La conférence des commissaires européens a vu le jour en 1994. Par ailleurs, depuis près de vingt ans, existe la conférence internationale des commissaires à la protection des données au sein de laquelle sont représentés une trentaine de pays.
(195) Le comité consultatif se compose, pour sa part, de représentants désignés par les États signataires eux-mêmes (voy. article 18, § 2, de la Convention n° 108).
(196) L'intervention du groupe doit être envisagée comme l'un des divers mécanismes tendant à garantir une approche commune en matière de flux à destination de pays tiers.
(197) En vertu de l'article 30, § 5, la Commission doit informer le groupes des suites réservées à ses avis et recommandations et rédiger à cet effet un rapport publié qui devrait être transmis au Parlement et au Conseil.

(198) Conventions ou futures conventions.
(199) Le point 42 de la résolution du Parlement européen sur le bilan 1996 et le programme 1997, votée le 11 décembre 1996, demande un système de supervision indépendant pour la protection des données personnelles par les institutions et organes de l'Union, ainsi qu'une réglementation générale contenant les conditions minimales et les principes fondamentaux de l'accès au public des documents européens.
(200) La directive fait cependant indirectement allusion à la création d'une telle autorité lorsqu'elle inclut dans la composition du groupe institué en vertu de son article 29, § 2, un représentant «de l'autorité ou des autorités créées pour les institutions et organismes communautaires».

(201) Voy. le considérant 66.
(202) Décision du Conseil du 13 juillet 1987 fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission, *J.O.C.E.*, 1987, n° L 197/34.
(203) Un traitement contenant des données inexactes est assurément illicite, mais n'implique pas forcément une faute du responsable du traitement, notamment si les États nationaux y voient le lieu d'une obligation de diligence et de prudence.

possibilité d'exonération concernant les seules causes étrangères[204] et l'évolution même de la disposition dans ses différentes versions[205] pourraient fonder l'idée de la mise en place d'une véritable présomption de responsabilité. Par contre, l'absence d'indications claires et précises en ce sens dans les différents documents officiels publiés, la référence pour certaines obligations au critère de diligence[206] et le considérant n° 55[207] inciteraient à penser que les États membres restent libres d'appliquer leurs règles de droit commun de la responsabilité en la matière.

93. – Enfin, l'article 24 impose aux États membres de prévoir des sanctions applicables en cas de violation des dispositions nationales prises en application de la directive. La nature de ces sanctions est laissée à leur libre appréciation, même si le considérant 55 rappelle que celles-ci doivent être appliquées à toute personne, tant de droit privé que de droit public, qui ne respecte pas les dispositions visées.

(204) Le considérant n° 55 vise explicitement la faute de la victime et le cas de la force majeure.
(205) Dans ses deux premières versions, la disposition ne permettait l'exonération du responsable du traitement que dans le seul cas où il parvenait à démontrer qu'il avait pris les mesures de sécurité appropriées pour respecter les exigences de l'actuel article 17 (sécurité). Ce faisant, l'alinéa 2 de la disposition commentée ne venait que préciser une exonération parfaitement logique dans un système de responsabilité basé sur la faute. Entre-temps, le Parlement européen avait proposé de faire disparaître cette exonération en la remplaçant par un système de responsabilité plus objective: «Le responsable des données indemnise la personne lésée pour tout dommage ou préjudice résultant d'un enregistrement de ses données personnelles incompatible avec les dispositions de la présente directive» (avis du Parlement du 11 mars 1992, *J.O.C.E.* n° C 94 du 13 avril 1992, p. 192). La dernière version de l'alinéa 2 de l'article 23 apparaît dès lors comme une voie médiane entre la version de la Commission et celle avancée par le Parlement européen.

IX. – CONCLUSION

94. – En définitive, la *ratio legis* de la directive du 24 octobre 1995 pourrait se résumer en peu de mots: laisser circuler librement les données sous protection rapprochée. En effet, pour permettre une libre circulation des données à caractère personnel dans le cadre du marché intérieur, il fallait veiller à une harmonisation des législations nationales de protection des données au regard des droits et libertés des individus. Il s'agissait premièrement de rapprocher entre elles des normes nationales en prévoyant un régime commun de protection. Mais il s'indiquait tout autant d'amplifier la protection des données à caractère personnel pour «rapprocher» l'individu de la maîtrise de son image informationnelle, appelée à voyager nettement plus vite que lui depuis les développements de la société de l'information.

95. – L'œuvre normative des institutions de la Communauté européenne s'est avant tout alimentée du terreau fourni depuis janvier 1981 par le Conseil de l'Europe. La Convention n° 108 adoptée sous l'égide de ce dernier avait effectivement inspiré des législations de protection des données dans la plupart des États membres. Nonobstant, la directive entendait aller au-delà des dispositions de la Convention n° 108 pour hausser le niveau de protection garanti par ce biais initial. Dans cette optique, elle précise les principes généraux établis par ladite Convention, comme la récurrente comparaison des deux textes opérée ci-avant s'est employée à le démontrer. *Ipso facto*, la directive perd un des atouts de la Convention n° 108 dont le caractère général permet la prise en compte des innovations technologiques successives. L'adaptabilité de la directive au progrès technologique, tel celui que constitue l'incontournable phénomène d'Internet, semble d'ailleurs dès à présent susciter des problèmes que seule une transposition évolutive des dispositions de la directive par les États membres pourrait résoudre[208].

96. – Enfin, la directive entend régler le sort des données à caractère personnel transmises aux États tiers. Ces données doivent bénéficier d'une protection adéquate au-delà des frontières de l'Union européenne pour franchir celles-ci. La protection adéquate pourrait faire de la directive, à terme, une référence normative dont les États tiers s'inspireraient pour la protection des données à caractère personnel qui ne seraient pas directement issues de la Communauté européenne. Cet effet d'engrenage (*spill over*) externe ne serait pas le moindre des mérites de la directive, du moins si l'on considère qu'il en va, *in fine*, des droits et libertés de tout individu, quel qu'il soit, où qu'il se trouve...

Marie-Hélène BOULANGER
Cécile de TERWANGNE
Thierry LÉONARD
Sophie LOUVEAUX
Damien MOREAU
Yves POULLET

(206) Voy. l'article 2, *d*, («toutes les mesures raisonnables doivent être prises pour que les données inexactes [...] soient effacées ou rectifiées»); l'article 17 relatif aux règles de sécurité paraît également viser une obligation de diligence.
(207) Ce considérant présente l'existence d'un recours juridictionnel et de sanctions comme un remède au non-respect par le responsable du traitement de la loi nationale prise en application de la directive, ce qui semble revenir à viser la faute du responsable du traitement.

(208) Voy. M.H. BOULANGER, C. DE TERWANGNE, «Internet et le respect de la vie privée», *op. cit.*

Examen de jurisprudence

CONTENTIEUX COMMUNAUTAIRE

La présente chronique couvre la période de début juillet 1996 à fin juillet 1997. Une année sans grand éclat jurisprudentiel. À signaler toutefois l'arrêt *Wiljo* qui consacre, de façon regrettable, selon nous, la subsidiarité du renvoi préjudiciel en appréciation de validité par rapport au recours en annulation dans la foulée de l'arrêté *TWD* (n° 28) et un arrêt intéressant du 10 juillet 1997 sur les mesures d'exécution conforme d'un arrêt d'annulation (n° 16).

Par ailleurs, la Cour confirme sa sensibilité à l'égard de la recevabilité des renvois préjudiciels tout en rappelant aux juridictions nationales son souci de coopération loyale dans le cadre de cette procédure.

Enfin, il faut signaler l'accroissement du nombre d'actions en référé et surtout de pourvois, les acteurs de la scène judiciaire européenne s'étant, semble-t-il, désormais familiarisés avec les règles relatives à un double degré de juridiction.

(1) *Bundesverband der Bilanzbuchhalter*, C-107/95 P, *Rec.*, p. I-947. Voy. aussi ordonnance du 3 juillet 1997, *Smanor SA*, T-201/96.

I. – LE RECOURS EN CONSTATATION DE MANQUEMENT (articles 169 à 171 du traité CE)

1. – Par arrêt du 20 février 1997, la Cour a confirmé, sans contestation possible, le pouvoir d'appréciation discrétionnaire dont dispose la Commission dans l'ouverture de la procédure de l'article 169[1]. Ce principe a notamment pour conséquence que les particuliers ayant déposé une plainte ne bénéficient pas de la possibilité de saisir le juge communautaire d'un recours contre la décision de la Commission de classer leur plainte.

Ceci, même si la Commission a reconnu la violation des articles invoqués. La Commission est donc seul juge de l'opportunité de déclencher un recours en manquement, indépendamment de la réalité ou de l'importance de l'infraction.

Dans ce même arrêt, la Cour se montre, en revanche, plus conciliante à l'égard du recours d'un particulier mettant en cause le refus de la Commission d'engager une procédure basée sur l'article 90, paragraphe 3, du traité CE. À ce propos, la Cour précise que: «Il ne saurait être exclu *a priori* qu'il puisse exister des situations exceptionnelles où un particulier ou une association constituée pour la défense des intérêts collectifs d'une catégorie de justiciables, a la qualité pour agir en justice contre un refus de la Commission d'adopter une décision dans le cadre de sa mission de surveillance prévue à l'article 90, paragraphes 1 et 3[2].» La Cour rejette toutefois, en l'espèce, cette possibilité au motif que le requérant avait demandé à la Commission d'adresser à la RFA une décision constatant qu'un acte législatif de portée générale était contraire au traité. La formulation utilisée par la Cour est extrêmement prudente et apparemment restrictive. Aussi cette jurisprudence devra-t-elle être précisée sur deux points: l'étendue du pouvoir d'appréciation de la Commission dans l'exercice de la mission de surveillance que lui confère l'article 90, paragraphe 3, et les conditions exigées d'un particulier pour qu'il puisse faire condamner le refus de la Commission d'agir en méconnaissance de cette disposition.

2. – L'étendue du contrôle qu'exerce la Commission dans la procédure de l'article 169, conformément à la tâche lui incombant en application de l'article 155 du traité CE, s'étend au respect, par les États membres, des mesures prises à la suite d'un accord international conclu par la Communauté qui, en vertu de l'article 228 de ce traité, lie les institutions et les États membres. «Le bon accomplissement de cette tâche par la Commission suppose que le pouvoir qu'elle tient de l'article 169 du traité et qui lui permet de saisir la Cour en cas de manquement par un État membre aux obligations qui lui incombent en vertu de l'accord, ne soit pas entravé[3].» La Commission peut donc agir en manquement même si les États membres sont préalablement convenus entre eux, par suite d'une consultation au sein du comité de l'article 113, de l'interprétation et de la portée des engagements souscrits par la Communauté dans le cadre de l'accord international en cause.

3. – Selon une jurisprudence constante, l'avis motivé détermine et fixe le cadre juridique du manquement. Ainsi, les modifications introduites dans la législation nationale sont sans pertinence pour statuer sur l'objet d'un recours en manquement, dès lors qu'elles n'ont pas été mises en œuvre avant l'expiration du délai imparti dans l'avis motivé[4].

L'existence d'un manquement doit donc être appréciée en fonction de la situation de l'État membre telle qu'elle se présentait au terme du délai fixé dans l'avis motivé[5].

(2) *Ibid.*, point 25, p. I-964.
(3) Arrêt du 10 septembre 1996, *Commission c. Allemagne*, C-61/94, *Rec.*, p. I-3989, sp. point 15, p. I-4012.
(4) Arrêt du 2 juillet 1996, *Commission c. Royaume de Belgique*, C-173/94, *Rec.*, p. I-3265. Voy. déjà, arrêt du 11 août 1995, *Commission c. Allemagne*, C-433/93, *Rec.*, p. I-2303.

4. – Dans l'affaire C-96/95, le gouvernement allemand invoquait l'irrecevabilité du recours au motif que la Commission n'aurait pas respecté la règle de l'identité des griefs entre la procédure précontentieuse et la procédure contentieuse. Le caractère rigoureux de cette règle, systématiquement rappelée par la Cour[6], et ayant parfois engendré des manœuvres dilatoires des États membres, a été, en l'occurrence, assoupli, la Cour se limitant à constater que la Commission n'avait pas réellement modifié les griefs avancés pour circonscrire les manquements[7].

II. – LE RECOURS EN ANNULATION (articles 173, 174 et 176 du traité CE)

A. – Le moment où le contrôle de la légalité doit se faire

5. – Dans une affaire mettant en cause la légalité d'un règlement (CE) portant retrait de concessions tarifaires au détriment de la société Opel Austria, quelques jours avant l'entrée en vigueur de l'accord EEE, le Tribunal, dans un arrêt de principe, a rappelé que, «dans le cadre d'un recours en annulation en vertu de l'article 173 du traité, la légalité de l'acte attaqué doit être appréciée en fonction des éléments de fait et de droit existant à la date où l'acte a été adopté[8]» et non pas au moment de son entrée en vigueur. Pour apprécier les éléments de fait et de droit à prendre considération, il convient de tenir compte du principe de bonne foi qui «est le corollaire, dans le droit international public, du principe de la protection de la confiance légitime qui, selon la jurisprudence, fait partie de l'ordre juridique communautaire[9]». Dès lors, dans une situation où les Communautés avaient déposé les instruments de ratification d'un accord international, en l'occurrence l'accord EEE, à une date (soit le 13 décembre 1993) précédant l'adoption du règlement en cause (soit le 20 décembre 1993), et où, dès ce moment, la date d'entrée en vigueur de cet accord (soit le 1er janvier 1994) était connue, les opérateurs économiques pouvaient se prévaloir du principe de la confiance légitime pour s'opposer à l'adoption, par les institutions, dans la période qui précède l'entrée en vigueur de cet accord, de tout acte contraire aux dispositions de celui-ci qui, après son entrée en vigueur, produisaient un effet direct dans leur chef[10]. Le Tribunal en conclut que, dès lors, l'examen de la légalité du règlement litigieux doit se faire par rapport aux dispositions de l'accord EEE qui, après l'entrée en vigueur de ce dernier, produisent un effet direct[11].

(5) Arrêt du 17 septembre 1996, *Commission c. Italie*, C-289/94, *Rec.*, p. I-4405.
(6) Cf. not. arrêt du 17 novembre 1992, *Commission c. Pays-Bas*, C-157/91, *Rec.*, p. I-5899; arrêt du 12 janvier 1994, *Commission c. Italie*, C-296/92, *Rec.*, p. I-1.
(7) Arrêt du 20 mars 1997, *Commission c. Allemagne*, C-96/95, *Rec.*, p. I-1653. Voy. aussi arrêt du 10 septembre 1996, *Commission c. Belgique*, C-11/95, *Rec.*, p. I-4115.
(8) Arrêt du 22 janvier 1997, *Opel Austria GmbH c. Conseil*, T-115/94, *Rec.*, p. II-39, point 87. Voy. déjà arrêt du 7 février 1979, *France c. Commission*, C-15/76 et C-16/76, *Rec.*, p. 321, point 7; arrêt du 22 octobre 1996, SNCF et *British Railways c. Commission*, T-79/95 et T-80/95, *Rec.*, p. II-1491, point 48.
(9) *Ibid.*, point 93. Voy. arrêt du 3 mai 1978, *Töpfer*, 112/77, *Rec.*, p. 1019, point 19.

B. – La notion d'acte attaquable

6. – Selon une jurisprudence constante, seules constituent des actes susceptibles de faire l'objet d'un recours en annulation, au sens de l'article 173 du traité CE, les mesures produisant des effets juridiques obligatoires de nature à affecter les intérêts des requérants, en modifiant de façon caractérisée leur situation juridique. Lorsqu'il s'agit d'actes dont l'élaboration s'effectue en plusieurs phases, ne sont attaquables que les mesures qui fixent définitivement la position de l'institution au terme de la procédure, à l'exclusion des mesures intermédiaires dont l'objectif est de préparer la décision finale.

Ainsi, ne saurait, tant par sa nature que par ses effets, être considérée comme un acte susceptible de recours, une décision de la Commission engageant une procédure antidumping. Il s'agit, en effet, d'un acte purement préparatoire qui n'affecte pas immédiatement et de manière irréversible la situation juridique de l'entreprise requérante[12].

7. – La notion d'acte attaquable est indifférente de la dénomination de l'acte en cause. Seule importe la prise en considération des critères dégagés par la jurisprudence.

Ainsi, une communication de la Commission peut présenter des caractéristiques l'assimilant à un acte attaquable au sens de l'article 173 du traité CE. Il en a été jugé ainsi par un arrêt de la Cour du 20 mars 1997 à propos d'une communication de la Commission relative à un marché intérieur pour les «fonds de retraite». Joignant l'examen de la recevabilité à celui du fond, la Cour procède à une analyse minutieuse des dispositions de la communication, pour conclure que celle-ci «constitue un acte destiné à produire des effets juridiques distincts de ceux déjà prévus par les dispositions du traité relatives aux prestations des services, à la liberté d'établissement et à la libre circulation des capitaux, en sorte qu'elle est susceptible de faire l'objet d'un recours en annulation[13].»

8. – En revanche, un recours en annulation dirigé contre un acte qualifié de «règlement», peut être déclaré irrecevable au motif que cet acte, après analyse, apparaît comme ne prévoyant qu'une offre aux producteurs (en l'espèce, les producteurs de lait et de produits laitiers) et ne produisant à leur égard aucun

(10) *Ibid.*, point 94.
(11) *Ibid.*, point 95.
(12) Ordonnance du Tribunal du 10 décembre 1996, *Söktas*, T-75/96, *Rec.*, p. II-1689, sp. points 26 à 31 et jurisprudence citée. Voy. aussi arrêt du 10 juillet 1997, *Oficemen*, T-212/95, point 53.
(13) *République française c. Commission*, C-57/95, point 23.