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

Journal des tribunaux
DROIT EUROPÉEN

Septembre 1997
n°41 - 5e année

BUREAU DE DÉPÔT: GENT X
MENSUEL, SAUF JUILLET/AOÛT

Editeur: LARCIER, rue des Minimes, 39 - B-1000 BRUXELLES

ISSN 0779-7656

Dossier

LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN DROIT COMMUNAUTAIRE

Deuxième partie*

27. – La détermination des finalités poursuit un objectif identique à l'exigence de prévisibilité de la loi imposée par la jurisprudence relative à l'article 8 de la Convention européenne des droits de l'homme. Il s'agit de circonscrire *a priori* l'étendue de l'atteinte à la vie privée en déterminant les limites dans lesquelles agit la personne qui s'ingère. Selon l'article 8 de la Convention, une atteinte à la vie privée, tel un traitement de données mis en œuvre par une autorité publique, doit être prévue par une loi qui en détermine les limites avec assez de netteté pour assurer à l'individu une protection contre l'arbitraire[64]. Un traitement de données mis en œuvre par les services de police n'est par exemple licite que si la loi qui l'autorise indique de manière suffisante en quelles circonstances et sous quelles conditions, la puissance publique est habilitée à opérer pareille atteinte secrète à la vie privée[65]. Ainsi, l'article 8 de la Convention n'autorise pas les écoutes téléphoniques à des fins de surveillance exploratoires ou générales[66].

L'obligation de détermination poursuit également un objectif de transparence: il ne peut y avoir de finalité dissimulée. La précision de la détermination devrait être appréciée *in concreto*, en fonction de ce que l'individu est raisonnablement censé connaître[67]. Le responsable du traitement doit avertir la personne concernée de la finalité du traitement avec d'autant plus de précision qu'il s'écarte de son activité habituelle. Ainsi, une banque ne pourrait se contenter d'affirmer qu'elle utilise les données relatives à ses clients «pour toutes les finalités légales en ce compris les finalités de marketing» alors qu'elle en fait usage à des fins de prospection d'assurance[68]. En effet, les activités d'assurance ne relèvent pas forcément des activités habituelles d'une banque et la personne concernée ne peut raisonnablement supposer que ses données seront utilisées à cette fin.

L'obligation de finalité déterminée vise enfin à permettre le contrôle de la légitimité du traitement et de la pertinence des données par une autorité de contrôle[69], que ce soit sur la base de la notification du traitement (cfr *infra*) ou à l'occasion d'une plainte.

b. – La finalité doit être légitime

28. – L'article 6, *b*, de la directive dispose en outre que les données doivent être collectées pour des finalités légitimes[70].

Le but même de la protection des données – le respect des libertés et des droits fondamentaux de l'individu – implique qu'une finalité de traitement ne peut violer sans justification légitime ces droits et libertés. C'est pourquoi la finalité poursuivie doit être utile et nécessaire au vu de l'objet social de l'entreprise ou de l'intérêt général. Elle ne peut non plus provoquer une ingérence excessive dans les libertés individuelles. Il convient en effet de mettre en balance l'intérêt des individus concernés à voir préserver leurs droits et libertés, et l'intérêt public ou privé à procéder au traitement des données.

L'application de la règle de proportionnalité doit permettre de vérifier que l'atteinte portée

(*) La première partie de cet article est parue dans notre précédente livraison: *J.T.D.E.*, 1997, pp. 121-127.

(64) Voy. Cour eur. D. H., arrêt *Malone* du 2 août 1984, précité, p. 32; et Cour eur. D. H., arrêt *Gillow* du 24 novembre 1986, série A, n° 109, p. 21.

(65) Cour eur. D. H., arrêt *Malone*, précité, p. 32; Cour eur. D. H., arrêt *Leander*, précité, p. 23, § 51.

(66) Cour eur. D. H., arrêt *Klass* du 6 septembre 1978, précité, p. 23, § 51.

(67) Voy. par exemple pour le degré de précision de la loi portant atteinte aux droits de l'homme: Cour eur. D. H., arrêt *Vereinigung Demokratischer Soldaten Österreich* du 19 décembre 1994, série A, n° 302, § 31; Cour eur. D. H., arrêt *Chorrer* du 25 août 1993, série A, n° 266 B, § 25.

(68) Anvers, 7 juin 1994, *D.C.C.R.*, 1994, p. 83 à 92, note Th. LÉONARD; *Computerrecht*, 1994, n° 4, p. 244, note J. DUMORTIER et F. ROBBEN; *D.I.T.*, 1994, n° 4, p. 51, note O. LESUISSE.

(69) M.-H. BOULANGER, C. DE TERWANGNE et Th. LÉONARD, *op. cit.*, p. 377; S. GUTWIRTH, *op. cit.*, p. 1443.

(70) Voy. l'article 5, *b*, de la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981.

SOMMAIRE

aux intérêts de la personne fichée ne soit pas excessive ou, à tout le moins, qu'elle soit compensée par la poursuite d'un intérêt supérieur du responsable du traitement[71].

29. – La notion de finalité légitime est à rapprocher de l'article 8, § 2, de la Convention qui prévoit qu'une atteinte à la vie privée doit être une mesure nécessaire dans une société démocratique, à l'un des objectifs que cette disposition énumère.

La Cour européenne des droits de l'homme considère que sont seules nécessaires dans une société démocratique les atteintes pertinentes et suffisantes[72]. Une atteinte à la vie privée est pertinente si elle est utile à la réalisation d'un des buts arrêtés par l'article 8, § 2, de la Convention: «Une ingérence inefficace par rapport au besoin social impérieux qu'elle était censée servir constitue une violation de la Convention»[73]. La suffisance implique qu'entre différentes mesures soit choisie la moins dommageable pour la vie privée. Une mesure pertinente et suffisante doit en outre être assortie de garanties. Transposé à notre matière, constitueraient notamment des garanties le fait que la durée d'un traitement, sa finalité, sa nécessité et sa pertinence soient déterminées[74]. Enfin, une atteinte, tout en étant pertinente, suffisante et assortie de garanties, ne peut apparaître disproportionnée[75].

Ces principes ont été reconnus dans la jurisprudence de la Cour de justice des Communautés européennes qui, se référant à l'article 8 de la Convention européenne de sauvegarde, a énoncé que des restrictions peuvent être apportées à la vie privée «lorsqu'elles répondent effectivement à des objectifs d'intérêt général et qu'elles ne constituent pas, au regard du but poursuivi, une intervention démesurée et intolérable qui porterait atteinte à la substance même du droit protégé»[76].

c. – La compatibilité des traitements avec les finalités

30. – L'article 6, *b*, énonce que «les données ne doivent pas être traitées ultérieurement de manière incompatible avec les finalités de la collecte». Aucun éclairage n'est apporté dans le texte même de la directive ou dans les considérants sur le sens à donner à cette disposition. L'article 5, *b*, de la Convention n° 108, qui comprend une règle identique, n'est guère plus explicite.

Au moins deux interprétations peuvent être proposées.

31. – Dès lors qu'une finalité est annoncée lors de la collecte, elle doit être respectée ultérieurement. Toute opération portant sur les données trouve en effet ses limites dans la finalité déterminée, explicite et légitime annoncée. La disposition n'est donc pas nouvelle. Elle est déjà induite dans le principe de finalité lui-même. On met ici en exergue une des conséquences essentielles du principe de détermination des finalités: si l'on traite les données de manière incompatible avec le but initialement annoncé, on poursuit une finalité distincte. Si cette nouvelle finalité n'est pas déterminée au vu et au su des personnes concernées ou des tiers, il y a un détournement de finalité. La règle n'empêche donc pas l'évolution ultérieure des traitements par rapport aux finalités annoncées lors de la collecte. On peut changer de finalité, mais alors, on doit y voir un nouveau traitement soumis intégralement à la réglementation.

Cette interprétation paraît conforme à une recherche de la *ratio* du texte commenté. Le sens ne peut être à trouver, vu l'objet de cette matière, que dans la protection recherchée pour la personne concernée par les données. L'idée semble être qu'il faut éviter que des données obtenues en annonçant une finalité particulière soient utilisées pour un tout autre but. On retrouve ici la crainte des détournements de finalités. Un détournement suppose que le changement de finalité soit opéré à l'insu de la personne concernée, sans que cette dernière puisse réagir. Le responsable du traitement doit donc toujours être attentif à faire connaître à la personne concernée les finalités réellement poursuivies sans en masquer l'une ou l'autre.

32. – Une autre interprétation pourrait également être soutenue. Plutôt que de n'autoriser que les utilisations des données qui s'inscrivent dans les finalités annoncées au moment de la collecte, sous peine de se trouver en présence d'un nouveau traitement (avec tout ce que cela implique comme formalités d'information, de notification, etc. cfr. *infra*), l'article 6, *b*, peut se lire comme admettant tous les changements de finalité compatibles avec les buts annoncés initialement, sans y voir la création de nouveaux traitements. Il faut toutefois rappeler que la finalité initiale doit être explicite, ce qui réduit considérablement l'étendue des finalités compatibles.

Pour appréhender la portée de la règle et éclairer davantage la notion de «compatibilité», on pourrait notamment se référer utilement à l'attente raisonnable des personnes concernées au vu de la finalité première. Une finalité de marketing de produits bancaires paraît ainsi incompatible avec une finalité d'évaluation du risque du crédit à accorder. Lorsque la personne fournit ses données pour l'évaluation du risque, elle ne s'attend pas raisonnablement à ce que les informations transmises puissent être automatiquement utilisées pour des finalités de prospection. Toute difficulté n'est toutefois pas écartée.

Ainsi, quel est le sort d'une nouvelle finalité réputée «compatible»? Autrement dit, la compatibilité permet-elle de faire l'économie d'un contrôle de légitimité appliqué au but nouvellement poursuivi? Si l'on répond par l'affirmative, on confisque à la personne concernée toute protection vis-à-vis de la nouvelle finalité. Ainsi, dans le cas où une communication des données à un tiers – opérée par exemple lors d'un échange de fichiers clientèles ou de membres d'une association – serait jugée compatible avec une finalité de gestion de la clientèle et de marketing des produits ou services offerts, la personne concernée ne pourrait plus s'opposer à la communication en contestant la légitimité de celle-ci. La compatibilité serait donc en quelque sorte un blanc-seing permettant d'éviter un contrôle de légitimité. Est-ce réellement le but des rédacteurs de cette disposition? Il est assurément permis d'en douter.

Par ailleurs, qu'advient-il des utilisations de données incompatibles avec les finalités annoncées lors de la collecte de celles-ci? Doit-on lire l'article 6, *b*, comme les interdisant purement et simplement? Cela figerait une fois pour toutes les finalités des traitements au moment de la collecte. Des données collectées par une société d'assistance à des personnes voyageant à l'étranger dans le but unique de gérer ce service ne pourraient pas être utilisées ultérieurement – suite à une diversification des activités – dans un but de marketing d'un nouveau produit d'assistance des personnes âgées. Une telle interprétation ne paraît pas raisonnable. Les traitements ne constituent généralement pas des fins en eux-mêmes, mais bien les supports d'activités économiques ou d'intérêt général. Ces activités doivent se transformer en fonction de l'évolution des besoins. S'y opposer sur la base de la protection des données est disproportionné par rapport à l'élément de protection recherché. Le fondement de la protection n'est pas à trouver dans le refus de changement des finalités, mais dans la nécessité de soumettre tous les traitements aux principes fondamentaux de la protection. L'important est donc d'éviter que la personne concernée ignore ces modifications et ne puisse, le cas échéant, s'y opposer. Il faut sans doute voir dans les utilisations incompatibles la mise en œuvre de traitements nouveaux générant l'ensemble des obligations liées à tout traitement en tant que tel.

33. – En conséquence, la transposition en droit interne d'une telle disposition suscitera vraisemblablement des débats sans doute difficiles. On ne peut à ce stade que regretter que les auteurs de ce texte n'aient pas franchement posé le problème des transformations de finalités, très fréquentes en pratique. C'est d'autant plus étonnant que certaines législations nationales, dont la loi belge, possédaient une règle particulière d'information dans cette hypothèse[77].

(71) Th. LÉONARD, Y. POULLET, «Les libertés comme fondement de la protection des données nominatives», in F. RIGAUX, *La vie privée une liberté parmi les autres?*, Travaux de la Faculté de droit de Namur n° 17, Bruxelles, Larcier, 1992, p. 250 et s.; S. Gutwirth, *op. cit.*, p. 1439 et s.

(72) Cour eur. D. H., arrêt *Dudgeon* du 30 janvier 1981, Série A n° 45, p. 28; Cour eur. D. H., arrêt *Sunday Times* du 27 octobre 1978, série A, n° 30, p. 38; Cour eur. D. H., arrêt *Olsson* du 24 mars 1988, série A, n° 130, p. 32.

(73) Cour eur. D. H., arrêt *Dudgeon*, précité, § 60.

(74) Cour eur. D. H., arrêt *Klass*, précité, p. 24.

(75) Voy. J.O. VIOUT, «La Cour européenne des droits de l'homme et le principe de proportionnalité», in *Le principe de proportionnalité en droit belge et français*, Liège, Éd. du Jeune Barreau de Liège, 1995, p. 187 et s. L'auteur n'hésite pas à qualifier le contrôle exercé par la Cour de contrôle de pure opportunité. Voy. aussi M.A. EISSEN, «Le principe de proportionnalité dans la jurisprudence de la Cour européenne des droits de l'homme», in L.E. PETTITI, E. DECAUX, P. A. IMBERT, *La Convention européenne des droits de l'homme*, *op. cit.*, p. 65 et s.

(76) C.J.C.E., 5 octobre 1994, précité (note 21).

(77) Article 9 de la loi du 8 décembre 1992; sur ce dernier, voy. M.-H. BOULANGER, C. DE TERWANGNE et Th. LÉONARD, *op. cit.*, p. 382.

34. – L'article 6, *b*, précise enfin que n'est pas réputé incompatible un traitement ultérieur à des fins historiques, statistiques ou scientifiques, pour autant que les États membres prévoient des garanties appropriées. Selon le considérant 29, les garanties appropriées doivent notamment empêcher les mesures ou décisions prises à l'encontre d'une personne sur base de ces traitements. Pour élaborer celles-ci, les États membres se réfèreront utilement à la future recommandation du Conseil de l'Europe sur la protection des données à des fins statistiques et au règlement communautaire relatif à la statistique communautaire[78].

C. – Les principes de qualité des données

35. – L'article 6, *c*, dispose que les données doivent être adéquates et pertinentes par rapport aux finalités[79]. On vise ici une liaison nécessaire et suffisante de l'information par rapport à la finalité. Il est vrai que, bien souvent, cette obligation rejoint le souci de rationalisation du responsable du traitement qui désire normalement ne conserver que des informations utiles à ses activités.

En pratique, un audit «protection des données», révèle que bon nombre de données sont seulement conservées ou enregistrées pas habitude alors qu'elles ne présentent par réellement d'utilité pour un traitement. Il convient alors de les supprimer. La règle va cependant plus loin. Ainsi, elle implique également qu'une donnée ne soit pas conservée dans le système si le but recherché peut être atteint autrement, par un moyen moins dommageable pour les libertés individuelles. Cela pourrait être le cas si l'identification d'une personne peut être garantie autrement que par la conservation d'un numéro d'identification nationale.

36. – Par ailleurs l'article 6, *c*, précise que les données ne doivent pas être excessives au regard de la finalité poursuivie. Seraient-elles adéquates et pertinentes, les données ne peuvent néanmoins pas faire l'objet d'un traitement si elles provoquent une atteinte disproportionnée aux intérêts de la personne concernée. Il peut s'avérer utile pour un organisme de crédit de traiter des données médicales relatives à des candidats à l'ouverture de crédit afin de sélectionner le risque; toutefois, un tel dévoilement d'informations touchant à l'intimité des individus peut s'avérer excessif. Seul le traitement de certaines données médicales pourra, le cas échéant, être justifié au vu de la nature et de l'ampleur des prêts envisagés.

37. – L'article 6, *d*, dispose que les données doivent être exactes et, si nécessaire, mises à jour[80]. Il précise que «toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement soient effacées ou rectifiées». Il s'agit donc clairement d'une obligation de moyens. Le critère à prendre en compte sera donc celui du responsable normalement prudent et diligent.

38. – Enfin, l'article 6, *e*, prévoit que «les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement»[81].

On retrouve ici ce qu'on appelle communément le droit à l'oubli de la personne concernée par les données. L'idée sous-jacente est qu'une donnée conservée pour une durée excédant un délai raisonnable peut être considérée comme non pertinente ou excessive eu égard à la finalité poursuivie.

D. – Les principes de légitimation des traitements

39. – L'article 6, *b*, impose que les finalités soient légitimes et que les données ne soient pas excessives par rapport à ces finalités. Il faut admettre que ces conditions abstraites – débouchant sur l'imposition d'un critère de proportionnalité – sont particulièrement difficiles à appréhender et peu éclairantes pour la plupart des responsables du traitement. C'est sur ce point que la directive vient innover en précisant explicitement les règles de base de la légitimation des traitements[82].

L'article 7 indique en effet des situations – les plus fréquentes en pratique – où la règle de proportionnalité est *a priori* respectée. Les traitements seront normalement admis s'ils trouvent leur fondement soit dans le droit privé – par un contrat (7, *b*) ou le consentement de la personne concernée (7, *a*) – soit dans le droit public –, par une obligation imposée par la loi (7, *c*) ou par la poursuite par l'État d'une mission d'intérêt public (7, *e*), soit enfin dans l'intérêt vital de la personne concernée (7, *d*). Un dernier fondement est l'intérêt prépondérant du responsable du traitement ou d'un tiers à qui sont communiquées les données (7, *f*). Dans le même temps, l'article 7 prévoit des conditions spécifiques assurant *a priori* un équilibre entre les intérêts de la personne concernée et du responsable du traitement.

En dehors de ces conditions, aucun traitement de données ne peut avoir lieu. La formule introductive de l'article 7 ne laisse pas aux États membres la latitude d'imaginer d'autres hypothèses ni d'exclure l'une d'entre elles[83]. Par contre, en vertu de l'article 5, ils sont libres d'être plus exigeants dans la formulation de l'une des hypothèses.

40. – Le traitement peut d'abord être poursuivi «si la personne concernée a indubitablement donné son consentement». Le consentement dont il s'agit doit bien évidemment répondre aux conditions contenues dans la définition donnée en préliminaire par la directive[84].

L'insertion de l'adverbe «indubitablement» permet d'admettre les consentements qui, sans nécessairement être exprès, n'en sont pas moins certains.

Le traitement se justifie également *a priori* s'il est «nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci».

Dans ce cas, le responsable devra s'assurer que le traitement est réellement nécessaire à la conclusion ou l'exécution du contrat, c'est-à-dire que la finalité du traitement vise l'essence même des mesures précontractuelles ou de l'objet des prestations. Sur cette base, une banque ne pourra pas forcément établir des profils de consommation de ses clients à partir de l'utilisation de leur carte de crédit, dans le cadre du contrat de fourniture du service.

La disposition permet aussi le traitement de données nécessaires au respect d'une obligation légale à laquelle le responsable du traitement est soumis. On peut citer à titre d'exemple des obligations qui s'imposent aux employeurs, telles la tenue d'une comptabilité particulière ou d'un registre du personnel accessible aux inspecteurs chargés du contrôle de la législation sociale, la communication de certaines données de leur personnel aux organismes de sécurité sociale, etc.

Le traitement des données est également permis s'il est «nécessaire à la sauvegarde de l'intérêt vital de la personne concernée». Le considérant 31 de la directive précise qu'on vise la protection d'«un intérêt essentiel à la vie de la personne concernée». Cette disposition pourrait fonder le traitement de données dans les cas où la personne concernée se trouve dans une situation d'urgence médicale[85].

Le traitement peut être aussi fondé s'«il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données

(78) Règlement n° 322/97 du Conseil du 17 février 1997 relatif à la statistique communautaire, précité.
(79) L'article 5, *c*, de la Convention n° 108 est libellé de manière identique.
(80) Cet article reprend le libellé de l'article 5, *d*, de la Convention n° 108.

(81) L'article 5, *e*, de la Convention n° 108 dispose également que «les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées». Le rapport explicatif de la Convention n° 108 souligne que cela ne signifie pas qu'elles doivent être séparées après quelque temps irrévocablement du nom de la personne à laquelle elle se réfèrent, mais seulement qu'il ne doit pas être possible de relier facilement les données et les identifiants.
(82) Le projet de recommandation du Conseil de l'Europe, relative à la protection des données à carectère personnel à des fins d'assurance reprend cette démarche en distinguant les conditions de licéite des conditions de légalité (voy. CJ-PD, [97] 28, p. 5).

(83) L'article 7 énonce que «les États membres prévoient que le traitement des données à caractère personnel ne peut être effectué que si [...]», suivent alors les différentes situations.
(84) Voy. *supra*, n° 20.
(85) Contrairement au traitement de données sensibles, le responsable ne doit pas prouver dans ce cas, que la personne concernée se trouvait dans l'incapacité physique ou juridique de donner son consentement (article 8, § 2, *c*).

sont communiquées». On vise ici les traitement poursuivis dans le secteur public au sens large. Si l'on effectue le rapprochement avec la règle de légitimité, on retrouve les principes administratifs de légalité, spécialité et proportionnalité[86]. Il arrive que dans la poursuite de ses missions prévues par la loi, l'administration soit amenée à porter atteinte aux libertés individuelles. Pareille atteinte doit être proportionnelle, c'est-à-dire suppose qu'une relation raisonnable existe entre le but poursuivi et les moyens mis en œuvre pour l'atteindre, ce qui est excessif devant être taxé non seulement d'inopportun, mais d'illégal[87]. Le principe de proportionnalité oblige l'autorité administrative d'une part, à examiner les intérêts en présence avant de prendre une décision – la motivation de la décision devant faire apparaître la mise en balance – et d'autre part, à prendre un acte conforme à cette balance[88].

Enfin, l'article 7 admet la mise sur pied d'un traitement s'«il est nécessaire à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée». Cette disposition diffère quelque peu des hypothèses précédentes. Alors que ces dernières précisaient des situations où l'équilibre des intérêts en présence est *a priori* respecté, la présente disposition rappelle de manière plus explicite le contenu même de la règle de proportionnalité inhérente au principe de légitimité. Même si le traitement est nécessaire au responsable, il ne pourra être poursuivi dès lors que l'opposition des intérêts en présence se résout en faveur de la personne concernée. Ce faisant, on perçoit encore mieux la nature explicative de l'article 7 qui a pour objectif principal d'éclairer le contenu des exigences du principe de légitimité des traitements.

41. – L'articulation entre les article 6 et 7 précités doit être bien comprise.

Le fait de remplir une des conditions de l'article 7 n'implique pas que l'exigence de légitimité de l'article 6, ni aucune autre de ses règles, soit *ipso facto* rencontrée. Les deux dispositions doivent au contraire s'appliquer cumulativement.

C'est ce que rappellent les considérants de la directive: tout traitement doit poursuivre une finalité légitime et respecter les autres exigences de l'article 6[89], mais pour être licite, il doit, en outre, être fondé sur une des situations reprises à l'article 7[90]. Si les règles de l'article 7 doivent être nécessairement respectées, les obligations qui en découlent ne permettent pas de faire l'économie de l'application des autres conditions de licéité contenues dans l'article 6. Ainsi, le consentement de la personne concernée ne permet pas nécessairement – même si ce sera souvent le cas – de légitimer la finalité du traitement[91].

Si l'on veut pousser plus avant la comparaison entre les deux dispositions, on pourrait dire que l'article 7 prévoit des situations abstraites dans lesquelles l'équilibre des intérêts en présence est normalement respecté, sans préjudice d'un contrôle concret, issu de l'article 6, permettant, le cas échéant, de révéler une atteinte inacceptable aux droits et intérêts de l'individu.

E. – Catégories particulières de traitement

42. – La directive prévoit des règles de protection particulières en ce qui concerne les traitements de certaines données dites «sensibles» (E.*a*) et les traitements se fondant sur la liberté d'expression (E.*b*).

a. – Les traitements de données «sensibles»

43. – Deux catégories de données font l'objet d'une réglementation particulière.

Tout comme l'article 6 de la Convention n° 108[92], l'article 8 de la directive part du principe que les traitements portant sur certaines données sont *a priori* interdits. Ces données sont limitativement énumérées. Un régime commun est établi pour celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle. On retrouve ici les données dites «sensibles» au sens le plus classique.

D'autres données ne peuvent être traitées que sous certaines conditions spécifiques. Certaines de ces conditions, très générales, sont déterminées par la directive, les autres sont laissées à la discrétion des États membres. Il s'agit des données relatives aux infractions, aux condamnations pénales ou mesures de sûreté, aux sanctions administratives, aux jugements civils ainsi que les numéros d'identification nationale ou autre identifiant de portée générale. On vise donc ici principalement les données dites «judiciaires».

44. – Le principe d'interdiction de traitement des données de la première catégorie souffre un grand nombre d'exceptions prévues précisément ou non par le texte même de la directive[93].

L'article 8, § 2, *a*, autorise le traitement de données sensibles «lorsque la personne concernée a donné son consentement explicite à un tel traitement»[94].

Les États membres disposent cependant d'une grande marge de manœuvre puisqu'ils peuvent prévoir que, dans les cas qu'ils déterminent, le consentement ne lève pas l'interdiction. On peut s'attendre à ce que les États membres optent pour une telle possibilité dans les nombreuses hypothèses où le consentement libre de la personne concernée est illusoire vu la nature particulière des relations entre celle-ci et le responsable du traitement: données sensibles relatives à un membre du personnel traitées par son employeur, données sensibles exigées par les assureurs ou tout autre prestataire d'un service devenu nécessaire économiquement ou socialement dans nos sociétés modernes, données sensibles traitées par une autorité publique, etc.

Le consentement doit répondre aux exigences de la définition arrêtée de manière générale par la directive[95]. Il doit en outre être explicite, mais ne doit pas forcément être donné par écrit.

L'article 8, § 2, *b*, lève l'interdiction de traiter des données sensibles si le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail[96].

En son point *c*, l'article 8, § 2, permet le traitement de données sensibles lorsque le

(86) Voy. Th. LEONARD, Y. POULLET, «Les libertés comme fondement de la protection des données nominatives», *op. cit.*, p. 242, n° 15 et 260, n° 43; il faut par ailleurs ne pas perdre de vue les exigences de l'article 8, § 2, de la Convention européenne des droits de l'homme.

(87) O. DAURMONT et D. BATSELE, «Cinq années de jurisprudence du Conseil d'État relative aux principes généraux du droit administratif», *Adm. publ.*, 1990, p. 274.

(88) P. LEWALLE, «Le principe de proportionnalité dans le droit administratif», *Adm. Publ.*, 1995, p. 53; R. ANDERSEN, «Le juge de l'excès de pouvoir et la mise en balance des intérêts en présence», in Ph. GÉRARD, F. OST, M. VAN DE KERKOVE, *Droit et intérêt*, Bruxelles, FUSL, 1990, p. 144.

(89) Considérant 28 de la directive.

(90) Considérant 30 de la directive.

(91) Le fait que l'article 6, *b*, de la directive parle de finalités légitimes et que l'article 7 soit intitulé «Principes relatifs à la légitimation des traitements de données» pourrait laisser croire le contraire (voy. également la version anglaise). Le texte néerlandais de la directive lève l'ambiguïté. En son article 6, il dispose que «De Lid Staten bepalen dat de persoonsgegevens voor een welbepaalde uitdrukkelijk omschreven en *gerechtvaardigde* doeleinde moeten worden verkregen [...]» alors que l'article 7 est intitulé «Beginselen betreffende de *toelaatbaarheid* van gegevensverwerking». Autrement dit, l'article 7 n'indique que des principe d'admissibilité du traitement sans préjudice des autres dispositions de la directive.

(92) Les catégories de données diffèrent cependant quelque peu. L'article 6 de la convention n° 106 n'inclut pas l'appartenaire syndicale.

(93) La convention n° 108 quant à elle, interdit le traitement de données sensibles à moins que le droit interne ne prévoie des garanties appropriées, cette dernière expression recouvrant les mesures protégeant les données sensibles qui vont au-delà de la protection minimale accordée aux données non sensibles (voy. CT-PD, [93] 5, p. 7).

(94) L'article 4.3, C, iii de la recommandation R (97) 5 relative à la protection des données médicales (précitée) dispose de manière similaire que «les données médicales peuvent être collectées et traitées si la personne concernée ou son représentant légal ou une autorité de contrôle ou toute autre personne ou instance désignée par la loi y a consenti, pour une ou plusieurs finalités et pour autant que le droit interne ne s'y oppose pas».

(95) Voy. *supra*, n° 20.

(96) Il est à noter que si les articles 4.3.b.iii et 7.3.b, iii de la recommandation R (97) 5 du Conseil de l'Europe relative à la protection des données médicales autorise leur traitement dans le cadre d'obligations contractuelles, l'alinéa 6 du point 74 de l'annexe à la recommandation précise que «lors du traitement de données dans le cadre des obligations contractuelles, les États membres de la Communauté ne pourront, après transposition de la directive communautaire dans leur législation nationale, faire usage de cette faculté que dans le contexte du droit du travail. Pour les autres membres du Conseil de l'Europe, ces dispositions peuvent entrer en ligne de compte dans d'autres domaines, tels que le sport, la formation ou les assurances».

traitement est nécessaire à l'intérêt vital de la personne concernée ou, dans les cas où cette dernière se trouve dans l'incapacité physique ou juridique de donner son consentement, d'une autre personne[97].

En vertu du point *d* de la même disposition, une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale peuvent également traiter des données sensibles si le traitement est effectué dans le cadre de leurs activités légitimes et avec des garanties appropriées, pour autant que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées. Cependant, seules les données sensibles relatives aux membres de ces organismes et aux personnes entretenant des contacts réguliers liés à la finalité du traitement sont visées. Cette exception paraît particulièrement vague. On peut se demander quelles pourraient être les garanties «appropriées» dont question dès lors qu'elle seraient différentes de celles prévues explicitement. On perçoit mal également comment déterminer les personnes liées à la finalité d'un traitement: n'est-ce pas toujours le cas des personnes concernées par les données?

Sont aussi visés par la levée de l'interdiction les traitements portant sur des données manifestement rendues publiques par la personne concernée et ceux nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice.

L'article 8, § 3, de la directive autorise finalement le traitement de données sensibles à des fins médicales (médecine préventive, diagnostic médical, administration de soins de santé ou de traitements) et à des fins de gestion des services de santé[98]. Si cette disposition permet le traitement de données sensibles dans le cadre de la relation thérapeutique, elle ne semble pas pouvoir couvrir les traitements de données dans les expérimentations médicales (essais cliniques de médicaments, essais d'appareils, etc.). En outre, il faut que le traitement soit effectué par un praticien de la santé soumis au secret professionnel, ou par une autre personne soumise à une obligation de secret équivalente.

L'article 8, § 4, permet également aux États membres d'autoriser, pour un motif d'intérêt public important, d'autres cas de traitements portant sur des données sensibles à condition que ces traitements soient accompagnés de garanties appropriées[99]. Le considérant 34 indique comme exemple de domaines où l'intérêt public pourrait justifier la levée de l'interdiction la santé publique et la protection sociale[100], la recherche scientifique et les statistiques publiques. On risque donc de voir apparaître dans ces matières des divergences importantes entre États membres.

45. – En ce qui concerne les données judiciaires, l'article 8, § 5, distingue selon la nature de celles-ci. Les données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peuvent être normalement traitées que sous le contrôle de l'autorité publique en prévoyant des garanties appropriées et spécifiques. Toutefois, les États membres peuvent prévoir des exceptions[101] et permettre, par exemple, que des sociétés privées, comme des banques ou sociétés d'assurances, traitent ces données s'ils prévoient des garanties particulières.

Les données judiciaires relatives aux sanctions administratives et civiles peuvent également être traitées sous le contrôle de l'autorité publique si l'État membre en décide. Le texte ne précise pas si des garanties appropriées et spécifiques doivent être arrêtées. Une interprétation littérale du texte implique que les États membres ne puissent permettre leur traitement en dehors du contrôle de l'autorité publique. On comprend mal ce qui justifie ici un régime plus strict que pour les données à caractère pénal.

La directive s'en remet enfin aux États membres pour prévoir les conditions dans lesquelles un numéro d'identification national ou tout autre identifiant de portée générale peut faire l'objet d'un traitement. On peut donc en conclure que ces données ne peuvent pas être utilisées en dehors d'une réglementation précise.

46. – Les difficultés qui surgiront lorsque les États membres devront transposer en droit interne les dispositions de l'article 8 sont en grande partie identiques à celles rencontrées antérieurement au sein de chaque État membre.

Le principe d'interdiction pose des problèmes insolubles de légistique. On a beau faire preuve de prévoyance en énonçant une kyrielle d'exceptions, la liste devra être indéfiniment complétée par des hypothèses où le traitement des données sensibles paraît légitime même si elles ne s'insèrent pas dans celles déjà arrêtées. La directive, malgré son effort de systématisation, n'évitera pas le même écueil.

La difficulté sera cependant encore plus aiguë dès lors que les possibilités laissées par l'article 8, § 4, aux États membres d'étendre les exceptions sont par essence limitées. Accroître les exceptions en dehors de la marge de manœuvre laissée aux États aurait pour conséquence d'amoindrir la protection désirée élevée ou de créer des brèches trop importantes à l'équivalence recherché des niveaux de protection.

Paradoxalement, certaines exceptions frappent par leur imprécision. On pourra alors être amené à profiter de celle-ci pour les interpréter de la manière la plus extensive en vue d'y insérer des hypothèses non expressément visées. Ce faisant, on permet à des traitements réellement problématiques de passer entre les mailles de la protection.

Un autre effet pervers risque enfin de se présenter. Afin d'étendre les exceptions, les États membres risquent de se contenter de lever l'interdiction par la voie du consentement dans des hypothèses où ce dernier est un leurre.

b. – Les traitements de données à caractère personnel et la liberté d'expression

47. – L'article 9 de la directive impose aux États membres de prévoir des exemptions et des dérogations aux principes fondamentaux de la protection mise en place «dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression». Dans le même temps, la disposition précise cependant que seuls sont visés «les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire».

Ces exemptions et dérogations ont, *a priori*, un champ d'application extrêmement large puisqu'en réalité, c'est la presque intégralité des règles de la directive qui peuvent ainsi être réduites à néant: les principes de licéité des traitements[102], les dispositions relatives au transfert de données à caractère personnel vers des pays tiers[103] et aux autorités de contrôle et groupe de protection[104]. En bref, parmi les règles directes de protection, seules les dispositions générales contenant les définitions et précisant le champ d'application de la directive ainsi que les règles relatives aux recours et sanctions ne peuvent être énervées au nom de la liberté d'expression.

48. – L'élan des États membres sera toutefois bridé par le critère de nécessité et la définition restrictive des finalités de traitements pour lesquels une exception à la protection est possible. Dans le cadre d'un commentaire général de la directive, trois seules réflexions seront faites sur ces limitations.

Les États membres ne peuvent *a priori*, au nom de la liberté d'expression, exclure du champ d'application de leur législation nationale les traitements visés par la directive, ni les soumettre entièrement à celle-ci. L'article

(97) Voy. *supra*, n°40.
(98) L'article 4.4. de la recommandation relative à la protection des données médicales précitée prévoit également que les données médicales puissent être traitées à des fins de gestion de service de santé. Il précise néanmoins que «la gestion est fournie par le professionnel de santé qui a collecté les données».
(99) Les dérogations au principe d'interdiction doivent toutefois être notifiées à la Commission.
(100) Le considérant 34 précise qu'il vise principalement les cas où il s'agit «d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie».
(101) Cette disposition précise qu'un recueil exhaustif des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.
(102) Chapitre 2 de la directive comprenant les dispositions relatives à la qualité des données (article 6), à la légitimation des traitements (article 7), aux données dites «sensibles» (article 8), à l'information de la personne concernée (articles 10 et 11), au droit d'accès (article 12), aux exceptions et limitations de l'article 13, au droit d'opposition de la personne concernée (articles 14 et 15), à la confidentialité et la sécurité des traitements (articles 16 et 17), à la notification, aux contrôles préalables et à la publicité des traitements (articles 16 à 21).
(103) Articles 25 et 26 de la directive.
(104) Articles 28 à 30 de la directive.

9 de la directive contient explicitement une obligation faite aux États de garantir un équilibre entre les deux libertés opposées.

La seule mesure de cet équilibre est à trouver dans la nécessité d'une conciliation entre les deux libertés concurrentes. Si des exceptions s'imposent d'elles-mêmes pour permettre l'exercice de la liberté d'expression – le secret des sources ne peut être réduit à néant par le droit à l'information reconnu à la personne concernée, le contrôle des journalistes ou entreprises de presse par les organes spécialement institués ne peut devenir l'instrument indirect d'une censure, etc. –, les principes de protection pourront être plus largement respectés une fois que la liberté d'expression a été pleinement exercée, c'est-à-dire une fois que les informations contenues dans les traitements ont été publiées ou mises à la disposition du public. On pense par exemple aux banques de données reprenant tout ou partie des informations publiées dans la presse écrite ou contenues dans des livres éditées.

La marge de manœuvre des États membres reste très importante. Ces derniers pourront tant jouer sur l'interprétation des finalités des traitements énoncées par le texte – qu'est-ce qu'une finalité journalistique? – que sur une interprétation propre du critère de nécessité lui-même. Un critère d'unification pourra cependant être utilement trouvé dans la jurisprudence de la Cour européenne des droits de l'homme afin de jauger le poids de chacune des libertés qui s'entrechoquent au travers de l'application des principes protecteurs de la directive.

IV. – LES DROITS DE LA PERSONNE CONCERNÉE ET LES OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

49. – Après avoir posé les principes de base de la protection de l'individu, la directive organise le contrôle de leur application. D'une part, elle garantit la transparence du traitement des données à caractère personnel par le biais de l'obligation d'information de la personne concernée, mise à charge du responsable du traitement (A). D'autre part, elle consacre différents droits pour la personne concernée lui permettant de conserver une relative maîtrise des données à caractère personnel la concernant. Les droits d'accès et de rectification retiendront d'abord l'attention (B). La directive introduit des exceptions générales à ces droits ainsi qu'à l'obligation d'information (C). Le droit d'opposition sera ensuite étudié (D). Enfin, la directive prévoit que la personne concernée ne peut être sujette à des décisions individuelles automatisées (E). Par ailleurs, une obligation de notification des traitements automatisés à l'autorité de contrôle nationale est instaurée (F) et des obligations de sécurité des traitements sont mises à charges des responsables du traitement (G).

50. – En principe, il appartient au responsable du traitement, voire à son représentant d'assurer le respect de ces droits et obligations. L'idée est d'élire un responsable unique du traitement, interlocuteur privilégié de la personne concernée.

A. – L'information de la personne concernée

51. – Le responsable du traitement a l'obligation d'informer la personne concernée sur les caractéristiques principales des traitements qu'il poursuit. Cette obligation permettra à la personne concernée d'exercer effectivement ses droits et de donner, le cas échéant, son consentement éclairé. Le respect de cette obligation d'information incombe au responsable du traitement ou à son représentant. Ces derniers sont toutefois dispensés de renseigner la personne concernée «lorsque [celle-ci] est déjà informée».

Les informations de base concernant l'identité du responsable du traitement[105] et les finalités des traitements devront toujours être transmises sauf si l'État membre fait application des exceptions générales prévues à l'article 13 de la directive. D'autres informations seront le cas échéant transmises à la personne concernée, selon les règles indiquées ci-après.

52. – Les modalités et l'objet de l'obligation d'information diffèrent selon que cette dernière est destinée ou non à une personne ayant directement transmis au responsable du traitement les données à caractère personnel la concernant.

Dans la première hypothèse, l'information se fera au moment même de la collecte auprès de la personne concernée[106]. En plus des informations de base, le responsable du traitement devra, le cas échéant, indiquer les destinataires ou catégories de destinataires des données, le caractère obligatoire ou facultatif des réponses ainsi que les conséquences d'un défaut de réponse, et mentionner l'existence des droits d'accès et de rectification des données.

Dans la seconde hypothèse, c'est-à-dire celle où les données n'ont pas été collectées auprès de la personne concernée, l'information devra être fournie dès l'enregistrement des données ou, si une communication des données à un tiers est envisagée, au plus tard lors de la première communication des données[107]. Les informations supplémentaires portent sur les destinataires ou catégories de destinataires des données, l'existence des droits d'accès et de rectification et les catégories de données concernées. Une exception particulière est ici prévue pour les traitements à finalité statistique et de recherche historique ou scientifique à condition que l'information de la personne concernée se révèle «impossible ou implique des devoirs disproportionnés, ou si la législation prévoit expressément l'enregistrement ou la communication des données». Dans ces cas, les États membres prévoient des garanties appropriées[108].

53. – En toute hypothèse, la directive précise que les informations supplémentaires ne seront transmises à la personne concernée que dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

Le texte de la directive ne spécifie pas quelles sont ces circonstances particulières. La loyauté doit être comprise au sens de l'article 6 de la directive, et renvoie dès lors à l'exigence de transparence. Les informations supplémentaires sont nécessaires dans la mesure où la personne concernée doit voir son attention attirée sur les risques spécifiques générés par le traitement en cause à l'égard de ses libertés individuelles (traitement de données sensibles, traitement de données dans le cadre d'un réseau ouvert, transmission de données vers des pays tiers n'assurant pas un niveau de protection adéquat, etc.)[109]. Ainsi par exemple, si les données sont destinées à être communiquées à des tiers autres que ceux auxquels la personne peut raisonnablement s'attendre, ceux-ci devront être spécifiés. C'est au responsable du traitement qu'il appartient dans un premier temps d'évaluer si la fourniture de telles informations est nécessaire, sous le contrôle en particulier des autorités nationales de protection des données.

Enfin, la directive reste muette quant à la procédure d'information elle-même. Il reviendra donc aux États membres de déterminer la forme qu'elle doit respecter (orale, écrite, collective, etc.).

B. – L'accès et la rectification des données

54. – Afin de contrôler la qualité des données la concernant (qu'elles soient complètes, exactes, mises à jour) et de vérifier le respect des règles découlant du principe de finalité, la directive confère à la personne concernée un droit d'accès aux données à caractère personnel se rapportant à elle[110]. Ce droit doit être exercé sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs.

La personne concernée doit ainsi pouvoir obtenir la confirmation que ses données personnelles sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées.

La personne concernée se voit également reconnaître le droit d'obtenir la communication, sous une forme intelligible, des données faisant l'objet du ou des traitements, ainsi que toute information «disponible» sur l'origine des données. Cette dernière obligation apparaîtra comme primordiale lorsque les données

(105) Le cas échéant, de son représentant (cf. article 10 de la directive).
(106) Article 10 de la directive.
(107) Article 11 de la directive.

(108) Article 11, § 2, de la directive. L'article 9, § 3, de la Convention n° 108 autorise également des restrictions au droit d'information pour les fichiers utilisés pour des recherches statistiques ou scientifiques «pour autant qu'il n'existe manifestement pas de risque d'atteinte à la vie privée».
(109) Voy. C. de Terwangne, S. Louveaux, «Data protection and on line networks», *Computer Law & Security Report*, 1997, vol. 13, n° 4.
(110) Article 12 de la directive.

n'ont pas été directement collectées auprès de la personne concernée[111].

55. – Du droit d'accès dérive le droit d'obtenir, selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la directive, notamment en raison de leur caractère incomplet ou inexact[112].

Ce droit de rectification est donc particulièrement étendu. Toutes les règles de la directive sont *a priori* visées sans exception: respect du principe de finalité, des règles de sécurité, de l'obligation de notification, etc. Le problème sera dès lors de veiller à une proportionnalité entre la gravité du manquement et la «sanction» demandée par la personne concernée. Il pourrait, par exemple, paraître insensé d'imposer l'effacement des données suite au non-respect de l'obligation de notification auprès de l'autorité de contrôle. Un verrouillage jusqu'à la mise en ordre du responsable du traitement paraîtrait par contre plus raisonnable.

La directive laisse la charge de la preuve des manquements à la personne concernée par les données, ce qui en pratique enlève à ce droit une grande partie de son contenu.

Le responsable du traitement doit, si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné, notifier aux tiers auxquels les données ont été communiquées les rectifications, effacements ou verrouillages effectués[113]. Le texte ne précise toutefois pas si le tiers est lui-même obligé de répercuter ceux-ci dans ses propres traitements[114].

C. – Exceptions communes

56. – L'article 13 de la directive autorise les États membres à limiter certaines obligations (principe de finalité légitime, droit d'information, droit d'accès) lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention et la poursuite d'infractions pénales, l'intérêt économique ou financier d'un État membre ou de l'Union européenne, et la protection de la personne concernée ou des droits et libertés d'autrui[115].

Cette liste correspond aux buts énumérés à l'article 8, § 2, de la Convention européenne des droits de l'homme, au nom desquels une atteinte à la vie privée des individus est admise. Selon l'article 8, § 2, de la Convention, une atteinte à la vie privée est justifiée si elle poursuit l'une de ces fins et est en outre strictement nécessaire dans une société démocratique, c'est-à-dire si elle est pertinente, suffisante et proportionnée au but légitime poursuivi[116]. A cet égard, l'article 13 soulève une question particulière car, en admettant explicitement que des données à caractère personnel soient traitées en dérogeant à l'exigence de finalité légitime (article 6, *b*, de la directive[117]), cette disposition ouvre la porte à des hypothèses dans lesquelles l'application du principe de proportionnalité pourrait être éludée.

57. – La portée exacte de l'article 13 de la directive dépendra en grande partie de ce que les États membres entendent par «la sûreté de l'État, la défense, [...] la protection des droits de la personne concernée ou des droits et libertés d'autrui».

Le considérant 42 de la directive précise à cet égard que «les États membres peuvent, dans l'«intérêt de la personne concernée ou en vue de protéger les libertés d'autrui, limiter les droits d'accès et d'information; ils peuvent, par exemple, préciser que l'accès aux données à caractère médical ne peut s'exercer que par l'intermédiaire d'un professionnel de la santé». Cette faculté laissée aux États membres d'introduire des limites au droit d'accès présente un grand intérêt. Un État pourrait, par exemple, autoriser des dérogations au droit d'information et au droit d'accès dans le but de permettre la prévention et la poursuite d'infractions pénales par le secteur privé (pour lutter par exemple, contre le vol dans les grands magasins, ou pour permettre à un gestionnaire de cartes de crédit de traquer les fraudes).

58. – L'article 13, § 2, évoque, par ailleurs, la possibilité pour les États membres de limiter par des mesures législatives les droits prévus à l'article 12 (à savoir le droit d'accès et de rectification) lorsque les données sont traitées exclusivement à des fins de recherche scientifique ou de statistiques. Cette possibilité doit s'accompagner de l'adoption par les États membres de «garanties légales appropriées»[118]. Il est toutefois exclu que les données puissent être utilisées dans ces cas aux fins de mesures ou de décisions se rapportant à des personnes précises

Ainsi, on pourrait imaginer que dans le cadre d'essais cliniques de médicaments, un État membre permette de ne pas communiquer les données à la personne concernée afin qu'elle ne puisse savoir si elle est véritablement sous médication ou sous placebo. Il en va de la crédibilité même de la recherche. Toutefois, cette limitation du droit d'accès devrait être limitée à la durée de la recherche effectuée à propos de la personne concernée.

D. – Le droit d'opposition

59. – L'article 14 de la directive reconnaît explicitement le droit pour la personne concernée de s'opposer pour des raisons prépondérantes et légitimes tenant à sa situation particulière à ce que des données la concernant fassent l'objet d'un traitement[119]. Si ce droit consacre *a priori* le droit pour tout individu de participer activement à l'utilisation de ses données, il convient toutefois d'en relativiser la portée. D'une part, libre cours est laissé aux États membres de prévoir des dispositions nationales contraires réduisant ou supprimant tout simplement ce droit[120]. D'autre part, afin de pouvoir s'opposer au traitement de ses données, la personne concernée doit invoquer des raisons «prépondérantes et légitimes tenant à sa situation particulière»[121]. Enfin, le droit d'opposition consacré par la directive ne revêt pas un caractère général. La personne concernée ne peut, en effet, s'opposer au traitement en lui-même mais uniquement au traitement de certaines données[122].

L'article 14 prévoit que le droit d'opposition doit exister au moins dans les cas visés à

(111) Cette obligation aura donc des implications importantes pour le secteur du marketing direct. La personne concernée qui reçoit un mailing d'une entreprise devra être renseignée sur l'identité du prestataire ayant confectionné les listes d'adresses. Ce dernier, questionné par la personne concernée, devra alors, le cas échéant, la renseigner sur ses sources d'approvisionnement. En Belgique notamment, où cette obligation n'existe pas encore, on remarque que c'est précisément la question de la source des données qui préoccupe souvent les personnes concernées par les données.

(112) Ces droits sont reconnus à l'article 8, *b* et *c*, de la Convention n°108.

(113) Il est à noter que l'article 12, § 3, de la loi belge prévoit que le maître du fichier doit communiquer les rectifications ou suppressions de données effectuées aux personnes auxquelles les données inexactes, incomplètes ou non pertinentes ont été communiquées, et ce pour autant qu'il connaisse encore les destinataires de cette information.

(114) La réponse à cette question devra être envisagée au cas par cas. Si, par exemple, le destinataire des données vient à connaître le caractère inexact d'une des données traitées, il commettrait une négligence fautive en ne corrigeant pas celle-ci. Par contre, le verrouillage suite à l'inexistence de mesures de sécurité adéquates dans le chef du communiquant n'aura normalement aucune conséquence de ce type.

(115) Voy. l'article 9 de la Convention n° 108 qui autorise également des dérogations aux obligations relatives à la qualité des données, aux traitement de données sensibles et aux droits de la personne concernée lorsque de telles dérogations constituent une mesure nécessaire dans une société démocratique à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État, à la répression des infractions pénales ou à la protection de la personne concernée et des droits et libertés d'autrui.

(116) Cf. *supra*, n° 29.

(117) Cf. *supra*, n° 28 où il est démontré que l'article 6, *b*, de la directive consacre le principe de proportionnalité.

(118) Voy. à ce sujet, la loi française n° 94-548 du 1er juillet 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.*, 2 juillet 1994, 9559.

(119) Ce droit n'est pas prévu dans la Convention du Conseil de l'Europe qui n'accorde à la personne concernée que le droit de demander l'effacement des données en cas de manquement aux articles 5 (qualité des données) ou 6 (principes régissant le traitement de catégories particulières de données). Par contre, la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (*J.O.*, 7 janvier 1978), prévoit en son article 26 que «toute personne a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement».

(120) L'on pourrait imaginer qu'un État membre ne reconnaisse pas ce droit lorsque la personne concernée a donné son consentement indubitable au traitement en question.

(121) La raison légitime ne doit pas, selon nous, être confondue avec l'existence ou non d'un fondement légitime au traitement des données trouvé dans l'article 7. Voy. *contra*, P. Mel, «The EC Proposed Data Protection Law», *Law and Policy in International Business*, vol. 25, 1993-1994, p. 316. Le critère retenu équivaut à une balance des intérêts à réaliser au niveau de l'individu.

l'article 7, points *e* et *f*, de la directive. Ce droit peut s'entendre comme une compensation de l'article 7, *f*, qui autorise le traitement de données au nom d'un intérêt légitime du responsable ou d'un tiers, pourvu que l'intérêt du sujet des données ne prévale pas. Même si un État membre refuse d'accorder un droit d'opposition pour la personne concernée[123], cette dernière pourra néanmoins contester la balance des intérêts sur base de l'article 7, *f*. Ce faisant elle s'opposera au traitement de ses données à caractère personnel en arguant d'un intérêt prépondérant et légitime, ce qui est cependant plus exigeant que ce que prévoit l'article 14, *a* (avancer une *raison* légitime prépondérante tenant à sa situation particulière).

60. L'article 14, *b*, consacre en outre un droit général et inconditionnel d'opposition dans le cadre du traitement de données à caractère personnel à des fins de prospection[124]. Dans ce cas, la personne concernée ne doit plus apporter la preuve d'une raison légitime afin de s'opposer au traitement de ses données. La directive opère à cet égard une distinction entre deux hypothèses:

– soit le responsable du traitement effectue lui-même une action de prospection; il doit alors offrir la possibilité pour la personne concernée de s'opposer gratuitement au traitement;

– soit les données sont traitées à des fin de prospection, non pas pour le compte du responsable lui-même mais pour le compte d'un tiers auquel les données sont éventuellement communiquées. Dans ce cas, le responsable est tenu d'informer la personne concernée et de lui offrir un droit de s'opposer gratuitement à ladite communication ou utilisation et ce avant même la communication au tiers ou l'utilisation des données par ce dernier.

E. – Décisions individuelles automatisées

61. – L'article 15 stipule que les États membres doivent prévoir le droit pour toute personne «de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.». Cette disposition vise donc à protéger la personne concernée contre le risque d'une utilisation abusive de l'informatique dans la prise de décision: «Le résultat fourni par la machine qui recourt à des logiciels de plus en plus sophistiqués, voire des systèmes experts, revêt un caractère apparemment objectif et incontestable auquel le décideur humain peut accorder une importance excessive, en abdiquant sa responsabilité»[125].

Trois conditions doivent être remplies afin de pouvoir invoquer l'article 15:

– premièrement, il doit y avoir un traitement tendant à une décision produisant des effets juridiques à l'égard de l'individu ou l'affectant de manière significative;

– deuxièmement, la décision doit être prise sur «le seul fondement» d'un traitement automatisé». Lorsque le processus de prise de décision contient une intervention humaine, l'article 15 ne pourrait être invoqué;

– troisièmement, le traitement automatisé de données doit être destiné à évaluer certains aspects de la personnalité de la personne concernée. Une décision qui n'a pas pour objet l'évaluation de la personnalité d'un individu déterminé ne tombe dès lors pas sous le coup de l'interdiction (le processus de décision d'autorisation de retrait d'argent d'un distributeur automatique, sur base du solde du compte, par exemple).

Les États membres peuvent néanmoins prévoir qu'une personne peut être soumise à une décision individuelle automatisée soit lorsque cette décision est prévue par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée; soit lorsque cette décision est prise dans le cadre d'un contrat, à la condition que la demande de conclusion ou d'exécution du contrat ait été satisfaite ou que des mesures appropriées (telles que la possibilité pour la personne concernée de faire valoir son point de vue) garantissent la sauvegarde de l'intérêt légitime de la personne. Dans le cas d'une telle décision, l'article 12 de la directive prévoit que la personne concernée doit pouvoir obtenir du responsable du traitement la connaissance de la logique qui sous-tend le traitement automatisé de données la concernant.

F. – La notification

62. – La directive établit en son article 18, § 1, le principe de la notification à adresser à l'autorité de contrôle, préalablement à la mise en œuvre d'un traitement[126]. L'obligation édictée porte sur les traitements entièrement ou partiellement automatisés ou les ensembles de tels traitements ayant une même finalité ou des finalités liées.

En règle générale, les réglementations actuellement en vigueur dans les États membres ne précisent pas le type de contrôle effectué à la réception de la notification. En pratique, cette dernière est fréquemment envisagée comme une formalité de publicité et n'est nullement assimilée à un système d'autorisation. Le contrôle à sa réception est bien souvent formel (rubriques non complétées, cohérence globale, etc.[127]) et n'empêche pas la mise en œuvre d'un traitement. L'examen de la licéité des traitements se situe plutôt *a posteriori*, sur base de la mise en cause du responsable du traitement, notamment en cas de plaintes émanant de particuliers. Bien entendu, dans ce cas, la notification constitue un élément d'appréciation important.

L'article 20 de la directive s'oriente partiellement dans une direction différente. Il impose aux États membres d'identifier *a priori* les traitements susceptibles de présenter des risques particuliers et de soumettre ceux-ci, préalablement à leur mise en œuvre, à l'examen de l'autorité de contrôle[128] ou du détaché à la protection des données[129]. En instaurant de cette façon un système de détermination préalable des traitements «à risques», la directive limite fortement le contrôle *a priori*[130]. Si l'on peut se rallier à une telle restriction en ce qui concerne ce type d'examen lorsqu'il est effectué par l'autorité de contrôle[131], elle paraît nettement plus contestable pour le détaché à la protection des données. En effet, c'est avant la mise en œuvre d'un traitement que la discussion la plus féconde peut avoir lieu. Dès lors que les traitements sont mis en œuvre, il est souvent délicat de les remettre en cause pour y intégrer des préoccupations de protection des données. A ce stade, la discussion est nécessairement plus polémique dans la mesure où des investissements importants peuvent avoir été réalisés et les pratiques déjà ancrées dans les mentalités des utilisateurs.

63. – L'article 19 de la directive précise le contenu minimum de la notification. Cette

(122) Article 14 de la directive: «En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne pourra plus porter sur *ces* données».

(123) Voy. *supra*, «sauf disposition nationale contraire».

(124) La directive ne précise pas que cette prospection doit être de nature commerciale, ainsi la prospection pour une œuvre caritative ou un parti politique tombe sous le champ de l'article 14 (voy. Exposé des motifs, COM [92] 422 final – SYN 287, p.27).

(125) Exposé des motifs, COM (92) 422 final – SYN 287, p.27

(126) Selon le considérant 48, cette obligation a pour objet d'organiser la publicité des finalités des traitements en vue de leur contrôle. A noter que bien que la Convention n° 108 ne contienne pas de disposition en ce sens, de nombreuses législations nationales ont mis en place des systèmes de notification des traitements de données (Autriche, Danemark, Espagne, Grand-Duché de Luxembourg, Portugal, Royaume-Uni, etc.).

(127) Voir la condamnation de la CNIL française pour refus de délivrance d'un accusé de réception (C.E. fr., 6 janvier 1997, *Caisse d'épargne Rhône-Alpes Lyon*, *A.J.D.A.*, 1997, n° 2, p. 206).

(128) Selon le considérant 54, la portée de l'intervention de l'autorité de contrôle devrait varier en fonction du droit national et prendre la forme soit d'une autorisation, soit d'un avis.

(129) L'article 20, § 3, de la directive précise qu'«en cas de doute», le détaché à la protection des données consultera l'autorité de contrôle.

(130) L'article 20, § 3, de la directive envisage un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées. Le considérant 53 mentionne diverses raisons pour lesquelles certains traitements pourraient présenter des risques particuliers, à savoir: leur nature, leur portée ou leur finalité, l'usage particulier d'une technologie. On peut penser, par exemple, à des traitements mis en œuvre par les pouvoirs publics et portant sur la totalité ou sur une proportion importante de la population ou à des traitements de données médicales. A noter que le considérant 54 laisse entendre que le nombre de traitements visés serait faible par rapport à l'ensemble de ceux qui sont mis en œuvre dans la société.

(131) Un examen préalable systématique ne conduirait, en effet, qu'à créer un système administratif extrêmement lourd qui s'accompagnerait inévitablement de délais d'attente avant la mise en œuvre de traitements (cfr *infra*).

dernière, envisagée comme un descriptif général, ne doit pas nécessairement faire apparaître tous les détails concrets du traitement, mais identifier le responsable du traitement, la ou les finalités de celui-ci[132], indiquer les (catégories de) personnes et de données concernées ainsi que les destinataires[133], et enfin les transferts vers les pays tiers et les mesures de sécurité adoptées. Afin d'assurer la publicité des notifications, l'article 21, § 2, prévoit la mise en place d'un registre accessible au public et reprenant l'ensemble des notifications introduites auprès de l'autorité de contrôle[134].

64. – De larges dérogations au principe de la notification obligatoire sont prévues, que ce soit sous forme d'exemption pure et simple ou de notification simplifiée[135]. Sur ce point, la directive laisse une grande autonomie aux États membres, tant en ce qui concerne la détermination des catégories de traitement qui ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes, que la possibilité de prévoir dans le droit national la désignation, par le responsable du traitement, d'un détaché à la protection des personnes chargé de garantir que les traitements concernés sont exempts de dangers[136].

La désignation d'un détaché à la protection des données agissant «en toute indépendance», paraît fort séduisante. Elle permettra d'échapper à la lourdeur administrative du système de notification[137], tout en garantissant la mise en œuvre de la législation au sein des organismes concernés. L'expérience allemande[138] en la matière s'est révélée très positive. Le détaché constitue un interlocuteur privilégié entre les organismes qui doivent mettre en œuvre la législation de protection des données et la ou les autorités qui en assurent le contrôle. Dans la mesure où il agit au sein même de l'institution, il est en mesure de veiller en connaissance de cause à la mise en pratique de la protection[139]. Ce faisant, il contribue fortement à l'intégration des règles par ceux qui sont censés les mettre en œuvre et complète de la sorte la tâche de l'autorité de contrôle. Enfin, il constitue, de par sa proximité, un interlocuteur facilement accessible pour les personnes concernées souhaitant faire valoir leurs droits. Il apparaît cependant essentiel pour qu'il puisse agir de cette manière que la législation nationale fixe son statut afin de garantir au mieux son indépendance[140].

G. – La confidentialité et la sécurité des traitements

65. – En vertu de l'article 17, § 1, de la directive, le maître du traitement a l'obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données[141]. Parmi les mesures techniques, on distingue les mesures de type physique, qui visent à protéger le système de la destruction par le feu, le gel, les pannes de courant, etc., des mesures de sécurité logiques, qui permettent de mettre en œuvre les principes de base de la protection des données[142].

Elles doivent permettre notamment que la collecte des données soit limitée aux données nécessaires, comme requis par l'article 6, *c*, de la directive, en empêchant que l'anonymat de la personne concernée ne soit levé sans nécessité[143]. Elles doivent également permettre que les données ne soient pas utilisées pour des finalités incompatibles, comme requis par l'article 6, *b*, en empêchant l'accès non autorisé aux données, ainsi que la lecture de celles-ci[144]. Elles doivent enfin permettre de garantir la fiabilité des données requise par l'article 6, *d*, en empêchant toute modification non autorisée des données.

À côté des mesures de sécurité techniques, les mesures de sécurité organisationnelles ou structurelles visent notamment à conscientiser le personnel au problème de la sécurité[145]. Parmi ce type de mesures, on mentionnera la nomination d'un détaché à la protection des données.

66. – L'article 17, alinéa 2, de la directive prévoit que ces mesures doivent assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données. Parmi les différents facteurs de risques relatifs aux données, on distinguera ceux relatifs aux données elles-mê-

(132) Voy. *supra*, point 15 en ce qui concerne la finalité comme critère de distinction des traitements. L'importance de la détermination de la finalité au moment de l'introduction de la notification ne doit cependant pas être sous-estimée car, en pratique, le responsable du traitement aura tendance à appliquer le principe de finalité sur base de celle-ci. L'expérience acquise au sein des États membres à cet égard montre que les responsables du traitement s'orientent généralement vers une description générique de la finalité. Dans ce cas, le contrôle peut difficilement s'exercer au regard du but global présenté, mais bien au regard des opérations particulières. Ainsi, pour un traitement défini sur base d'une finalité de gestion du personnel, on pourrait accepter l'emploi de données médicales en vue de la participation au remboursement de soins par l'employeur, mais leur utilisation pour d'autres objectifs spécifiques s'intégrant dans la finalité définie en termes larges (par exemple comme critère pour accorder ou non une promotion) doit être mise en cause.

(133) À comparer avec l'article 1, § 4, de la recommandation R (87) 15 du Conseil de l'Europe relative aux données de police qui précise que la nature du fichier, l'organe responsable du traitement, les finalités de ce dernier, le type de données contenues et les destinataires auxquels les données sont communiquées doivent être déclarés.

(134) Certains pays, comme le Royaume-Uni et la Belgique, envisagent la mise à disposition de ce registre public sur Internet.

(135) La directive permet également aux États de prévoir une dérogation ou une simplification de l'obligation en faveur des traitements visés à l'article 8, § 2, *d*. Par ailleurs, en l'état actuel, différents pays ont déjà mis en place des systèmes permettant d'alléger les formalités de notification. Ainsi, la Belgique et les Pays-Bas ont soustrait à cette obligation bon nombre de traitements supposés moins risqués. La France a opté pour le régime des déclarations simplifiées dans lequel le responsable du traitement s'engage à mettre en œuvre un traitement en respectant les normes simplifiées définies par l'autorité de contrôle.

(136) Aux termes de l'article 18, § 2, le détaché à la protection des données sera notamment chargé d'assurer l'application interne des dispositions nationales et la tenue d'un registre des traitements effectués par le responsable du traitement. Cette dernière obligation s'apparente à ce que l'on retrouve à l'article 16, § 1, de la loi belge du 8 décembre 1992 qui impose au maître du fichier de rédiger un «état» du traitement.

(137) Censée assurer la transparence des traitements tant vis-à-vis du grand public (via le registre public) que des autorités de contrôle, la notification préalable constitue une formalité administrative particulièrement lourde dont l'intérêt en termes de protection des individus et en particulier la valeur informative, peut être sérieusement mis en doute. Son principal (et unique?) avantage est de devoir être adressée à une instance externe – l'autorité de contrôle. Elle constitue dès lors un incitant pour les responsables de traitement à se familiariser aux règles de protection de données, les amenant notamment à s'interroger sur la légitimité et la pertinence des traitements qu'ils mettent en œuvre. La notification peut également former l'occasion privilégiée de nouer un dialogue entre les responsables des traitements (ou leurs organisations sectorielles) et les autorités de contrôle.

(138) *Datenschutzbeauftragter* ou «DSB» très répandu tant dans le secteur privé où sa désignation est obligatoire que dans le secteur public où elle ne l'est pas toujours. Le délégué à la protection des données bénéficie, en vertu de l'article 36 de la loi fédérale allemande du 20 décembre 1990, d'une protection particulière tendant à renforcer l'efficacité de la fonction. En particulier, dans l'exercice de ses compétences en matière de protection des données, il ne reçoit d'instructions de personne. Il ne peut être désavantagé en raison de l'accomplissement de sa mission. L'organisation à laquelle il appartient doit l'assister dans l'accomplissement de sa mission et lui garantir l'accès nécessaire aux dossiers. Il est soumis au secret professionnel.

(139) Le 49e considérant précise que le détaché peut être ou non employé par le responsable du traitement.

(140) On ne peut, en effet, totalement exclure le risque que les caractéristiques du détaché à la protection et notamment son appartenance à l'institution où les traitements sont mis en œuvre ne lui permettent pas de réaliser sa tâche en toute indépendance.

(141) L'article 7 de la Convention n° 108 prévoit une disposition similaire. Voy. aussi, pour des mesures de sécurité spécifiques, l'article 4 de la directive RNIS, précitée, l'article 8 de la recommandation R(87)15, précitée, concernant les données de police, l'article 13 de la recommandation R(89)2, précitée, relative aux données utilisées à des fins d'emploi, l'article 8 de la recommandation R(90)19, précitée, relative aux données utilisées à des fins de paiement, l'article 6 de la Recommandation R(95)4, précitée, relative aux données utilisées dans les télécommunications.

(142) Voy. le commentaire de la recommandation R(97)19, précitée, l'article 126 de la Convention d'application de Schengen, et la recommandation R(97)5 du Conseil de l'Europe relative à la protection des données médicales, qui dressent une liste type des mesures de sécurité logiques.

(143) Sur le principe de l'anonymat et les techniques des protecteurs d'identité (ou *Privacy Enhancing Technology*), cf. J.-Ph. WALTER, «La protection des données à l'heure des inforoutes», Brig, Séminaire Multimédia du 25 avril 1997, organisé par l'Association suisse de révision interne, p. 9.

(144) On vise ici les techniques de cryptage, de codage et de chiffrement. Il semble à l'heure actuelle qu'une clef de 128 bits offre un niveau de sécurité suffisant (*idem*).

(145) Cfr point 72 de la recommandation R(90)19, précitée.

mes (nature des données, nombre des données, nombre de personnes concernées, etc.), ceux concernant les finalités (nature de la finalité, multiplicité de finalités poursuivies par le traitement, finalité informative ou décisionnelle), ceux touchant à la nature de la relation juridique entre la personne concernée et le responsable du traitement, etc. Parmi les facteurs de risque relatifs au traitement, on mentionnera la structure interne du traitement, la multiplicité des utilisateurs, la multiplicité des localisations du traitement entraînant un accroissement des risques d'effraction (la localisation à un seul endroit augmentant, quant à elle, les risques liés à l'effraction), la technologie du traitement (les données contenues en réseau auquel chaque utilisateur peut accéder présentent plus de risques que celles traitées par un ordinateur personnel non connecté).

67. – L'article 17 précise que les mesures doivent être adéquates au regard de l'état de l'art et de la technique[146]. C'est donc une conception nécessairement évolutive du niveau de sécurité qui est prônée, en relation avec l'évolution technologique dans le domaine.

La directive impose des obligations de sécurité supplémentaire aux responsables de traitement qui recourent à un sous-traitant: ils sont en effet tenus de choisir un sous-traitant qui apporte des garanties suffisantes du point de vue de la sécurité. En outre, le contrat qui les lie doit être rédigé par écrit et prévoir que le sous-traitant n'agit que sur instruction du responsable du traitement.

L'article 16 généralise ce dernier principe en disposant que toute personne agissant sous l'autorité du responsable du traitement ou du sous-traitant ne peut, sauf obligation légale contraire, traiter ces données que sur instruction du responsable du traitement[147].

V. – LES FLUX TRANSFRONTIÈRES DE DONNÉES

68. – Si la directive entend rechercher une équivalence de protection des données à caractère personnel dans les différents États membres, elle s'attache également à régler le problème du droit national applicable à la réalité réglementée. La détermination du droit applicable est particulièrement nécessaire eu égard au développement de la dimension de plus en plus internationale des traitements de données à caractère personnel.

Tant que les données ne quittent pas le territoire de la Communauté, les règles de détermination de la loi nationale applicable sont censées suffire pour sauvegarder le niveau de protection des personnes concernées. La difficulté est alors d'éviter que le régime protecteur soit réduit à néant dès que ces données sortent du territoire européen tant il est vrai que la dimension internationale des flux d'informations, y compris nominatives, rendrait vaine l'existence d'une réglementation dont l'effectivité couvrirait le seul territoire européen. Les autoroutes de l'information que préfigure la toile d'Internet favoriseront encore cette circulation sans frontières, qu'il s'agisse de flux liés à la mobilité des personnes, de flux liés à un commerce électronique croissant ou à la consultation de sites étrangers, de flux, enfin, liés à des transmissions à l'intérieur d'un groupe d'entreprises, d'un secteur ou intersectoriels.

Les règles par lesquelles la directive tente de répondre à cette réalité font l'objet du commentaire qui suit. L'article 4, 1, *a*, permet de déterminer la loi nationale applicable et, par là, permet d'appréhender le régime des flux intracommunautaires de données (A). La directive assortit également de conditions les flux de données hors Europe (articles 25 et 26) et soumet, exceptionnellement, le responsable situé hors du territoire européen aux prescrits de la directive européenne (article 4, 1, *c*) (B)[148].

A. – Les flux transfrontières intracommunautaires

69. – Les auteurs de la directive sont partis du principe qu'un traitement ne devait normalement être soumis qu'à l'application d'une seule législation nationale[149].

Le critère de la localisation physique du traitement, retenu à l'origine, a été détrôné par celui du lieu de l'établissement du responsable du traitement. Vu la dimension internationale des traitements, ceux-ci auraient en effet été localisés dans chacun des États où une opération particulière était effectuée.

Le principe est énoncé à l'article 4, 1, *a*, de la directive. Si un traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement, la loi nationale applicable est celle du lieu où cet établissement est situé. L'établissement sur le territoire d'un État membre «suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable»[150]. La forme juridique retenue n'est donc pas déterminante: simple succursale, filiale ayant la personnalité juridique, etc.

70. – On peut se demander si le critère retenu permettra toujours d'éviter une application de plusieurs législations au même traitement. Un cas simple est celui où plusieurs sociétés distinctes, établies sur des territoires différents, décident de créer un traitement commun: elles sont chacune considérées comme responsables du traitement. En application de la règle générale, chacune de leur loi nationale s'applique au traitement en cause.

Le responsable du traitement peut avoir différents établissements stables sur le territoire européen. Dans ce cas, la même disposition énonce qu'il «doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable». La justification de cette solution semble être à trouver d'une part dans l'idée d'application de la loi la plus proche de la personne concernée, ce qui devrait permettre à cette dernière de demander l'application de la loi qu'elle connaît le mieux et pour laquelle elle est le mieux armée à en exiger l'application et d'autre part, dans la volonté d'éviter un contournement de législation[151].

Ici encore, on en arrivera à une application possible de plusieurs lois nationales au même traitement. On pense au cas où un traitement centralisé en un lieu déterminé dessert différentes sociétés d'un même groupe délocalisé sur plusieurs États membres.

En toute hypothèse, les solutions pourront encore être rendues plus complexes dès lors que des États interprètent différemment les notions de traitement ou de responsable, intervenant dans la mise en œuvre du critère de rattachement.

71. – Si seules des lois nationales des États membres sont applicables aux traitements en cause, aucune difficulté ne devrait plus survenir lors de flux transfrontières de données intracommunautaires. En effet, le principe inscrit à l'article 1, 2, de la directive interdit toute restriction ou interdiction apportée à la libre circulation des données au nom de sa loi nationale.

C'est peut-être oublier le problème de la marge de manœuvre laissée aux États membres dans la confection de leur législation nationale. En effet, on a vu que le principe de l'article 1, 2, était fondé sur l'idée de l'existence d'une protection équivalente dans les différents États membres du fait du rapprochement des législations nationales prises en conformité avec la directive. Vu la large marge de manœuvre laissée à ceux-ci à de nombreux niveaux de la protection, des traitements seront interdits par certains États et permis par d'autres. Par exemple, la Belgique interdit le traitement d'un certain type de données sensibles sauf si l'on obtient le consentement de la personne concernée alors que les Pays-Bas conservent l'interdiction complète de traitement en application de l'article 8, 2, *a*. Il s'agit assurément d'un cas de disparité entre législations nationales permise par la directive. Si une société établie en Belgique veut commercialiser ces données aux Pays-Bas, ses clients potentiels qui y sont établis devront refuser le transfert sous peine d'être en infraction avec leur propre loi nationale: la collecte de telles données y est illicite. Ce faisant, les Pays-Bas restreignent la libre circulation des données entre deux États membres. On touche là à une contradiction essentielle trouvant sa source dans la directive elle-

(146) Le paragraphe 117 de l'annexe de la recommandation R(97)5 précise que les mesures de sécurité devraient être à la hauteur des développements technologiques des systèmes d'information sans pour autant donner lieu à des dépenses démesurées. Comp. avec l'article 4, § 2, de la directive RNIS qui requiert que les mesures de sécurité soient prises «compte tenu des possibilités techniques les plus récentes».

(147) Ces deux dernières dispositions ont leur équivalent dans la Convention n° 108.

(148) Nous reviendrons *infra* sur la combinaison de ces différents articles.

(149) Exposé des motifs, précité, p. 12.

(150) Voy. considérant n°19.

(151) Voy. considérant n°19.

même. Dans l'exemple précité, les Pays-Bas respectent le prescrit de la directive concernant les données sensibles. La société belge peut par contre en appeler à l'article 1, 2, pour exiger que le flux de données envisagé soit autorisé.

Deux interprétations sont alors permises. La première consiste à admettre que les divergences entre les législations nationales, dans la mesure où elles se situent dans les limites de la marge de manœuvre laissée aux États membres, participent néanmoins à un niveau de protection équivalent de sorte que le refus du flux soit interdit. Pour que ce principe conserve une véritable portée, il faut alors admettre que le destinataire des données puisse continuer à traiter les données reçues nonobstant la règle contenue dans sa loi nationale. L'exigence de protection serait donc toujours équivalente à celle contenue dans la loi nationale la plus laxiste. L'autre consiste à admettre le refus du flux comme exception à l'article 2, 1, dès lors que sa *ratio* n'est pas respectée, mais c'est alors aller au-delà du texte de cette disposition. On peut gager que cette difficulté devra impérativement trouver une solution rapide au niveau communautaire sauf à enlever une grande portée au résultat de l'adoption de la directive commentée.

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

La suite et la fin de l'article paraîtront dans la livraison d'octobre 1997.

Examen de jurisprudence

LA SÉCURITÉ SOCIALE DES PERSONNES QUI SE DÉPLACENT À L'INTÉRIEUR DE LA COMMUNAUTÉ – ANNÉE 1996 –

1. – Avertissement du chroniqueur: *«Décider c'est choisir; choisir c'est sacrifier.»*

C'est un lieu commun que de souligner la technicité extrême des dispositions du règlement (CEE) n° 1408/71 du Conseil, du 14 juin 1971, relatif à l'application des régimes de sécurité sociale aux travailleurs salariés, aux travailleurs non salariés et aux membres de leur famille qui se déplacent à l'intérieur de la Communauté, tel que coordonné par le règlement (CEE) n° 2001/83 du Conseil, du 2 juin 1983[1], ci-après dénommé «le règlement», et du règlement (CEE) 574/72 qui en fixe les modalités d'application.

Cette caractéristique contraint presque naturellement celui qui procède à l'examen, pour une période donnée, de la jurisprudence de la Cour de justice CEE sur les questions préjudicielles relatives à l'interprétation des dispositions du règlement, à rappeller les principes fondateurs de celui-ci, les mécanismes principaux qu'il met en place, et à revenir sur des décisions prononcées au cours de périodes antérieures pour créer une mise en perspective des arrêts commentés, qui leur donne tout leur sens.

Prenant ici le relais, pour 1996, d'auteurs aussi brillants et renommés que S. Van Raepenbusch et V. Bertrand[2], j'ai fait le choix d'inscrire la présente chronique dans la continuité de leurs examens de la jurisprudence de la Cour et de renvoyer le lecteur au rappel des principes qu'ils développèrent à cette occasion, l'une et l'autre, avec brio.

Plus modestement, je propose au lecteur de lui présenter dans l'ordre chronologique où ils furent prononcés les neuf arrêts que la Cour de justice consacra au règlement.

Examen ou... chronique de jurisprudence, ce texte aura souvent, comme il se doit, le ton du récit; mon souhait est de ne pas effaroucher celui qui voudra bien m'accompagner dans l'analyse de ces décisions et de proposer, pour celles-ci, un accès qui soit certes rigoureux, mais engageant.

La matière est en effet austère, mais son importance pratique ne cesse de croître[3].

2. – Arrêt du 1er février 1996 – *Naruschawicus*[4].

Détermination du droit applicable – Bénéfice des prestations de chômage.

Mme Naruschawicus avait été occupée pendant 10 ans au service des Forces belges en Allemagne; elle résidait dans ce pays mais, comme fonctionnaire, conservait son domicile légal en Belgique et l'État belge versait les cotisations de sécurité sociale à l'ONSS.

Au moment de la rupture du contrat, le ministère de la Défense nationale la considéra fictivement et rétroactivement comme salariée et lui délivra les documents destinés à lui permettre de bénéficier des allocations de chômage.

Elle s'inscrivit donc comme demandeuse d'emploi et se prêta aux contrôles périodiques, mais continua de résider en Allemagne. L'ONEm lui refusa dès lors le bénéfice des allocations de chômage au motif qu'elle n'était pas disponible pour le marché de l'emploi.

La cour du travail de Liège, dans un arrêt du 15 novembre 1994, posa à la Cour de justice trois questions préjudicielles dont deux peuvent retenir notre attention:

- Elle demanda tout d'abord si la requalification *a posteriori* de la relation de travail avait une influence sur l'application des dispositions du règlement permettant de déterminer le droit applicable: si oui, Mme Naruschawicus devait être considérée comme salariée et le droit allemand lui était applicable puisque c'est en Allemagne qu'elle avait travaillé[5]; si non, Mme Naruschawicus demeurait fonctionnaire et le droit belge lui était applicable[6].

La Cour de justice décida que la requalification rétroactive était sans incidence sur la nature statutaire de la relation de travail[7]; le droit belge demeurait donc applicable.

- La cour du travail de Liège demanda en outre si le fait de résider dans un autre État membre que l'État compétent caractérisait une indisponibilité pour le marché de l'emploi dans ce second État.

La Cour répondit en décidant que l'inscription comme demandeur d'emploi et la soumission aux contrôles périodiques des services de l'État compétent suffisent à considérer que le travailleur concerné est disponible pour le marché de l'emploi et a donc droit aux allocations de chômage à charge de cet État[8].

3. – Arrêt du 28 mars 1996 – *Moreno*[9].

Bénéfice des prestations familiales pour les membres de la famille d'un chômeur.

M. Moreno, ressortissant espagnol, travaillait depuis 26 ans en Allemagne lorsque son employeur rompit le contrat de travail moyennant le paiement d'une indemnité.

Le droit allemand étant applicable, l'institution compétente pour le paiement des allocations familiales dues pour les deux enfants de

(1) *J.O.C.E.*, L 230, 6.
(2) Qui proposèrent respectivement les examens de jurisprudence pour la période de mai 1992 à avril 1994 (*J.T.D.E.*, 1994, 105-110) et l'année 1995 (*J.T.D.E.*, 1996, 153-161).
(3) On pourra, pour s'en convaincre et le cas échéant prolonger l'analyser, lire avec fruit deux récents articles parus au *J.T.T.* de 1997: S. Van Raepenbusch, «Le champ d'application personnel du règlement (CEE) n° 1408/71 et la citoyenneté européenne: du travailleur migrant au citoyen européen», 1-7; R. Cornelissen, «Résultats et limites du règlement (CEE) n° 1408/71», 209-216.
(4) C-308/94, *Rec.*, 1996, I, 207.
(5) Article 13, § 2, *a*, du règlement.
(6) Article 13, § 2, *d*, du règlement.
(7) Elle rappela cependant que le statut de fonctionnaire ne fait pas obstacle à ce que les personnes concernées soient rangées dans la catégorie des travailleurs salariés pour l'application d'autres dispositions du règlement (voir en ce sens C.J.C.E., 24 mars 1994, *Van Poucke*, C-71/93, *Rec.*, I, p. 1101, points 17 et 18).
(8) Voir en ce sens C.J.C.E., 27 mai 1982, *Aubin*, 227/81, *Rec.*, 1991, point 20.
(9) C-243/94, *Rec.*, 1996, I, 1887.