# Traité établissant une Constitution pour l'Europe

## Partie II
## La Charte des droits fondamentaux de l'Union
### Commentaire article par article

*Sous la direction de*

Laurence BURGORGUE-LARSEN
Anne LEVADE
Fabrice PICOD

Tome 2

EXTRAIT

BRUYLANT
BRUXELLES
2005

# ARTICLE II-68

PAR

OLIVIER DE SCHUTTER

PROFESSEUR À L'UNIVERSITÉ DE LOUVAIN-LA-NEUVE
ET À LA NEW YORK UNIVERSITY,
COORDINATEUR DU RÉSEAU UE D'EXPERTS INDÉPENDANTS
EN MATIÈRE DE DROITS FONDAMENTAUX

## ARTICLE II-68 – PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

**1. Toute personne a droit à la protection des données à caractère personnel la concernant.**

**2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.**

**3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.**

### Bibliographie

G. BRAIBANT, *La Charte des droits fondamentaux de l'Union européenne*, Paris, Seuil, 2001, p. 111; U. BRÜHANN, «La protection des données à caractère personnel et la Communauté européenne», *RMCUE* n° 428, 1999, p. 328; P. DE HERT et S. GUTWIRTH, «Controletechnieken op de werkplaats : herbeschouwing in het licht van persoonsgegevensbeschermingsrecht», *Oriëntatie* 1993, n° 5, p. 127; O. DE SCHUTTER, «Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel», *RTDH* n° 45 (2001), p. 137; G. DE VEL, «Le Conseil de l'Europe, la vie privée et la protection des données», *in* Y. POULLET, C. DE TERWANGNE et P. TURNER, *Privacy : new risks and opportunities*, Diegem, Story-Scientia, 1997, p. 21; F. MAIANI, «Le cadre réglementaire des traitements de données personnelles effectuées au sein de l'Union européenne», *RTDE* 2002, n° 2, p. 283; V. PORRO, «Il garante europeo della protezzione dei dati personali : il commento», *Giornale di diritto amministrativo* 2003, n° 1, p. 75; A. DE SÁ E MELLO, «Tutela juridica das bases de datos», *Direito da sociedade da informação* 1999, p. 111.



### Sommaire



**1.** L'article II-68 de la Constitution européenne puise son inspiration à l'article 8 de la Convention européenne des droits de l'homme, à la Convention du Conseil de l'Europe du 28 janvier 1981 *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, ainsi surtout qu'à un important acquis du droit de l'Union européenne – aussi bien primaire que dérivé – en matière de protection des données à caractère personnel. Comprendre la portée de l'article II-68 de la Constitution européenne suppose, par conséquent, d'examiner les apports de ces différents textes, bien que leur examen approfondi ne puisse être envisagé dans le cadre du présent commentaire.

**2.** Auparavant pourtant, il faut attirer l'attention sur deux questions d'interprétation.

Premièrement, les *explications* de la Charte établies sous la responsabilité du *Praesidium* ne font pas figurer l'article 8 de la Charte des droits fondamentaux de l'Union européenne (II-68) parmi les dispositions qui, aux fins de l'application de l'article II-112, paragraphe 3, de la Constitution européenne («*Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention*»), sont considérées comme ayant le même sens et la même portée que les articles correspon-

dants de la CEDH (v. CHARTE 4473/00 CONVENT 49 du 11 octobre 2000, version révisée, pour le français, CHARTE 4473/1/00 CONVENT 49 REV 1 du 19 octobre 2000; les *explications* mises à jour dans le cadre du Groupe de travail II de la Convention européenne (CONV 828/03, 9 juillet 2003) n'apportent sur ce point aucune modification). Ceci naturellement ne signifie pas que la jurisprudence de la Cour européenne des droits de l'homme, déjà riche en ce domaine et appellée à se développer encore à l'avenir, puisse être ignorée dans la lecture de l'article II-68 de la Constitution européenne. Si un doute devait subsister sur ce point, il serait aussitôt levé par la référence à la «clause de protection» de l'article II-113 de la Constitution européenne, dont l'effet est d'exclure toute interprétation de celle-ci qui aboutirait à diminuer le niveau de protection déjà acquis en vertu, notamment, des instruments internationaux de protection des droits de l'homme qui sont obligatoires à l'égard de l'ensemble des Etats membres.

**3.** Une seconde question d'interprétation concerne le rapport de l'article II-68 de la Constitution européenne à la législation européenne, c'est-à-dire au droit dérivé des institutions de l'Union. La mise à jour des *explications* adjointes à la Charte qui a été opérée au sein du groupe de travail II de la Convention sur l'avenir de l'Europe (CONV 828/03, 9 juillet 2003) comprend une référence à l'article I-51 de la Constitution européenne. Intitulé «*Protection des données à caractère personnel*», cet article dispose que «*1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. La loi ou loi-cadre européenne fixe les règles relatives à la protection des personnes physiques s'agissant du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes*».

**4.** Nous sommes ainsi témoins d'un renvoi en cascade, qui est source de confusion dans le rapport que le législateur européen entretient à la Constitution : les explications relatives à l'article II-68 de la Constitution européenne renvoient à une autre disposition constitutionnelle, mais celle-ci, à son tour, renvoie au législateur européen le soin de définir les modalités suivant lesquelles la protection des données à caractère personnel sera assurée. Ceci ne signifie cependant pas que le législateur européen deviendrait libre d'agir selon son bon vouloir, dès lors qu'il lui reviendrait de définir l'étendue de cette protection qu'il est tenu, par ailleurs, d'assurer. Il est plus adéquat de considérer que les principes régissant la matière de la protection des données à caractère personnel engagent le législateur européen, bien qu'il revienne à celui-ci, dans les limites fixées par ces principes, d'en définir les modalités d'application dans l'ordre juridique de l'Union; que le droit dérivé communautaire ait pu largement contribuer à l'identification de ces principes ne constitue pas à cet égard un obstacle.



## I. – L'apport du droit du Conseil de l'Europe

**5.** Les données à caractère personnel ne s'entendent pas uniquement des données relatives à la vie privée, mais comprennent toutes les données relatives à des personnes que ces données identifient, ou qui sont identifiables à partir de ces données. L'article 2, *littera* a, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (*JOCE* L 281 du 23 novembre 1995, p. 31; dir. modifiée par le règlement (CE) n° 1882/2003, *JOUE* L 284 du 31 octobre 2003, p. 13) précise que «*est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale*».

Le principe suivant lequel toute personne a droit à la protection des données à caractère personnel la concernant a sa source d'abord dans la Convention *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, conclue dans le cadre du Conseil de l'Europe le 28 janvier 1981 (S.T.E., n° 108; cette convention est entrée en vigueur le 1er octobre 1985). Tous les Etats membres de l'Union européenne ont ratifié cette convention. Des amendements à la Convention *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* ont été adoptés par le Comité des Ministres du Conseil de l'Europe lors de sa 675ième réunion, le 15 juin 1999, de manière à permettre l'adhésion des Communautés européennes. L'ensemble des Etats

parties doivent notifier leur acceptation desdits amendements pour que ceux-ci puissent entrer en vigueur et, seulement après leur entrée en vigueur, les Communautés européennes peuvent adhérer à la Convention.

Selon son Préambule, cette convention visait à «*étendre la protection des droits et libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés*». En effet, lorsqu'au milieu des années 1970 des préoccupations commencèrent à se faire jour quant aux menaces que faisaient peser sur la vie privée le développement des systèmes informatiques – facilitant le traitement automatisé des données, et dès lors également les échanges de telles données et les comportements discriminatoires pouvant s'y trouver liés – l'article 8 de la Convention européenne des droits de l'homme paraissait n'offrir qu'une protection relativement insuffisante. Il n'était pas acquis à l'époque – il n'est acquis que depuis peu – que cette disposition de la Convention européenne des droits de l'homme offre également une protection à l'individu à l'égard du *traitement des données à caractère personnel le concernant*, que ces données soient relatives à sa vie privée ou à des activités publiques.

**6.** Encore plusieurs années après l'adoption de la Convention n° 108, la Commission européenne des droits de l'homme conclut à l'absence d'ingérence dans la vie privée des requérants qui se présentaient à elle lorsque les renseignements collectés à leur propos – bien que constituant sans nul doute des données à caractère personnel au sens précité – ne renfermaient pas des «*données relatives à la vie privée*» (Comm. EDH, déc. du 9 septembre 1992, *F. Reyntjens c/ Belgique*, req. n° 16810/90, *D.R.* 73, p. 136, à propos d'un contrôle d'identité impliquant l'enregistrement des données figurant sur la carte d'identité) ou bien, comme lorsqu'une personne se trouve photographiée ou espionnée par vidéosurveillance alors qu'elle prend part à une manifestation publique ou se trouve dans un espace public (Comm. EDH, déc. du 12 octobre 1973, *X c/ Royaume-Uni*, req. n° 5877/72, *Ann. Conv.*, 16, p. 328; Comm. EDH, déc. du 7 décembre 1992, req. n° 18395/91, non publiée, citée par K. Rogge, «The Protection of Private Life and Technological Challenges», *Bull. dr. h.*, 2 (1994), p. 17, spec. p. 23), là où il apparaissait que l'intéressé ne tenait manifestement pas à préserver la confidentialité



des données recueillies à son propos. Le traitement de données à caractère personnel pouvait être examiné au regard de l'article 8 de la Convention européenne des droits de l'homme uniquement pour autant que les données aient été recueillies par des moyens constitutifs d'une ingérence dans la vie privée de l'individu, ou que celui-ci ait voulu préserver les données traitées de toute divulgation (Comm. EDH, déc. du 4 mai 1979, *X c/ Autriche*, req. n° 8170/78, *D.R.* 16, p. 145, spec. p. 160).

**7.** Même l'arrêt *Leander c/ Suède*, rendu par la Cour européenne des droits de l'homme le 26 mars 1987 (série A n° 116), bien qu'il soit généralement présenté comme opérant une évolution au sein de l'article 8 de la Convention européenne des droits de l'homme vers une protection étendue à tout traitement de données à caractère personnel, avait laissé subsister un certain doute. Cette affaire concernait un charpentier qui avait été écarté d'un poste impliquant de pouvoir circuler sur une base navale militaire, après que la police ait fourni sur lui certains renseignements permettant d'évaluer le danger que pourrait représenter son embauche du point de vue de la sécurité nationale. L'arrêt du 26 mars 1987 conclut à l'applicabilité de l'article 8 de la Convention en constatant que «*Le registre secret de la police renfermait sans contredit des données relatives à la vie privée de M. Leander. Tant leur mémorisation que leur communication, assorties du refus d'accorder à M. Leander la faculté de les réfuter, portaient atteinte à son droit au respect de sa vie privée, garanti par l'article 8, §1*». Pourtant la question de savoir de quelle nature étaient les renseignements transmis par la police à propos de M. Leander était demeurée ouverte jusqu'au terme de la procédure, le requérant ayant jusqu'au bout «*continué d'ignorer la nature des renseignements secrets consignés sur lui*»; et, bien qu'il ait exposé aux organes de surveillance de la Convention ses liens avec le Parti communiste suédois et avec plusieurs organisations syndicales, il est d'autant moins établi que ce soient ces activités qui aient été consignées par la police dans le registre secret tenu par elle que la réglementation applicable à l'époque précisait que ne pouvait figurer dans ce registre «*aucune mention (...) pour la simple raison que l'intéressé a exprimé une opinion politique par son appartenance à une organisation ou d'une autre manière*». L'on notera d'ailleurs que par la suite, lorsque la Commission européenne des droits de l'homme prendra appui sur la jurisprudence *Leander*, elle soulignera

que la nature *privée* des informations figurant sur le registre en cause constituait l'élément décisif dans cette affaire (Comm. EDH, rapp. du 13 novembre 1987, *Gaskin c/ Royaume-Uni*, req. n° 10454/83, §86; déc. du 9 juillet 1991, *Yvonne Chave c/ France*, req. n° 14461/88, *D.R.* 71, p. 141, spec. p. 148, sur des renseignements concernant l'internement psychiatrique dont l'intéressée avait fait l'objet; déc. du 6 juillet 1988, *I. Hilton c/ Royaume-Uni*, req. n° 12015/86, *D.R.* 57, p. 108, spec. p. 128 : «*La Commission ne considère pas qu'un contrôle de sécurité constitue en soi une ingérence dans le droit au respect de la vie privée, garanti par cette disposition. Une telle ingérence ne se produit que lorsque les contrôles de sécurité se fondent sur des informations touchant à la sphère privée de l'individu*»; déc. du 14 janvier 1998, *Herbecq et al. c/ Belgique*, req. n° 32200/96 et n° 32201/96, à propos du défaut de protection de la loi contre la vidéosurveillance : «*Les faits susceptibles d'être observés ne peuvent* (...) *essentiellement être que des comportements publics. Le requérant n'a pas non plus démontré de manière plausible que des comportements privés commis en public auraient pu faire l'objet d'une quelconque surveillance*»).

**8.** Finalement, c'est seulement récemment, dans l'arrêt *Rotaru c/ Roumanie* rendu le 4 mai 2000, que l'article 8 de la Convention européenne des droits de l'homme a été interprété par la Cour européenne des droits de l'homme comme englobant les garanties de la Convention n° 108 du 28 janvier 1981 (Cour EDH 4 mai 2000, *Rotaru c/ Roumanie*, req. n° 28341/95, *série A, n° 2000-V*). L'affaire avait sa source dans une information erronée transmise par le service roumain des renseignements, l'erreur ayant été commise en raison de l'homonymie du requérant avec une personne ayant milité dans les rangs du mouvement «légionnaire» d'extrême droite. L'information selon laquelle Aurel Rotaru avait eu un passé fasciste avait, dans un premier temps, conduit à le priver d'un décret-loi accordant certains droits aux personnes ayant été persécutées par le régime communiste. Lorsque la vérité fut rétablie, M. Rotaru n'en avait pas moins subi une atteinte grave à sa réputation, dont il rechercha sans succès réparation devant les juridictions roumaines. La Cour européenne des droits de l'homme constate l'applicabilité de l'article 8, paragraphe 1er, de la Convention à cette situation; faisant référence à l'arrêt *Leander* précité, elle rappelle «*que la mémorisation dans un registre secret et la communication de données relatives à la 'vie privée' d'un individu entrent dans le champ d'application de l'article 8, §1*». Rejetant l'argument du gouvernement selon lequel les informations transmises par le service roumain des renseignements sont relatives à des activités publiques imputées au requérant – sortant, par conséquent, du champ de la protection que confère le droit au respect de la vie privée –, la Cour réitère que «*le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de 'vie privée' (arrêts Niemietz c/ Allemagne du 16 décembre 1992, série A n° 251-B, p. 33, §29, et Halford c/ Royaume-Uni du 25 juin 1997, Recueil 1997 III 1015-1016, §§42 à 46)*». Elle note en outre avoir «*déjà souligné la concordance entre cette interprétation extensive et celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, entrée en vigueur le 1er octobre 1985, dont le but est 'de garantir* (...) *à toute personne physique* (...) *le respect* (...) *notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant' (article 1), ces dernières étant définies dans l'article 2 comme 'toute information concernant une personne physique identifiée ou identifiable' (Cour EDH 16 février 2000 Amann c/ Suisse [GC], req. n° 27798/95, §65). En outre, des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics. Cela vaut davantage encore lorsque ces données concernent le passé lointain d'une personne*».



**9.** La Convention n° 108 *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* n'a donc été englobée que par touches successives au sein de l'article 8 de la Convention européenne des droits de l'homme, et d'une manière qui demeure incomplète; ceci sans doute justifie que les *explications* adjointes à la Charte des droits fondamentaux ne considèrent pas que les clauses figurant respectivement à l'article 8 de la Convention européenne des droits de l'homme et à l'article 8 de la Charte des droits fondamentaux (II-68 de la Constitution européenne) soient «correspondantes» l'une à l'autre, ainsi qu'on l'a noté plus haut. Cependant, même avant de faire l'objet de cette incorporation au moins partielle dans l'article 8 de la Convention européenne des

droits de l'homme, la Convention n° 108 avait profondément influencé le développement du droit de l'Union européenne. Non seulement les Etats membres ayant adhéré à la Convention d'application de l'Accord de Schengen du 14 juin 1985, relative à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990, ont dû ratifier la Convention n° 108 du Conseil de l'Europe afin de rassurer leurs partenaires quant aux garanties entourant le traitement des données à caractère personnel, mais, en outre, le rapprochement des législations nationales dans ce domaine s'est imposée comme une mesure d'accompagnement indispensable de l'établissement du marché intérieur.

### II. – L'apport du droit communautaire dérivé

**10.** En vue de faciliter la libre prestation des services transfrontière tout en garantissant le maintien d'un degré élevé de protection de la vie privée à l'égard des traitements de donnnées à caractère personnel, le législateur communautaire a en effet adopté la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*. Cette directive a pour base juridique l'article 95 du traité CE (ex-art. 100 A TCE), disposition relative au rapprochement des législations nationales en vue de l'établissement du marché intérieur. En effet, ainsi que l'exprime le préambule de la directive, «*les différences entre États membres quant au niveau de protection des droits et libertés des personnes, notamment du droit à la vie privée, à l'égard des traitements de données à caractère personnel peuvent empêcher la transmission de ces données du territoire d'un État membre à celui d'un autre État membre; (...) ces différences peuvent dès lors constituer un obstacle à l'exercice d'une série d'activités économiques à l'échelle communautaire, fausser la concurrence et empêcher les administrations de s'acquitter des responsabilités qui leur incombent en vertu du droit communautaire*» (7ème cons.). L'article 1er de la directive énonce du reste très clairement qu'à la suite de son adoption, les États membres ne pourront restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel, le souci



de protection des droits fondamentaux de la personne constituant, selon la Cour de justice des Communautés européennes, un motif impérieux d'intérêt général susceptible de justifier des restrictions aux libertés fondamentales de circulation à condition que ces restrictions respectent les exigences de proportionnalité et de non-discrimination (CJCE 25 juillet 1991, *Commission c/ Pays-Bas*, C-353/89, *rec.* I 4089, pt 30; 25 juillet 1991, *Stichting Collectieve Antennevoorziening Gouda e.a. c/ Commissariaat voor de Media*, C-288/89, *rec.* I 4007, pt 23; 3 février 1993, *Vereniging Veronica Omroep Organisatie c/ Commissariaat voor de Media*, C-148/91, *rec.* I 513, pts 9 et 10; 26 juin 1997, *Familiapress*, C-368/95, *rec.* I 3689, pt 24; 12 juin 2003, *Schmidberger*, C-112/00, *rec.* I 5659, pts 76-77). Il s'agissait, par l'adoption de cette directive, d'éviter que les Etats membres n'entravent l'échange de données transfrontières en invoquant la nécessité de protéger l'individu du risque que les données le concernant ne bénéficient pas, dans d'autres Etats, d'un même niveau de protection. L'établissement d'un seuil élevé de protection à travers l'Union va donc de pair avec une obligation de reconnaissance mutuelle de la protection de la vie privée qu'assure chacun des Etats; c'est en cens que la directive 95/46/CE constitue, à la fois, un important instrument visant à la protection des droits fondamentaux et un puissant atout dans la création d'un espace sans frontières intérieures (ainsi que l'exprime encore le préambule de la directive (3ème cons.), «*l'établissement et le fonctionnement du marché intérieur dans lequel, conformément à l'article 7 A du traité, la libre circulation des marchandises, des personnes, des services et des capitaux est assurée, nécessitent non seulement que des données à caractère personnel puissent circuler librement d'un État membre à l'autre, mais également que les droits fondamentaux des personnes soient sauvegardés*»).

#### A. – *L'interprétation de la directive 95/46/CE*

**11.** La nature de la directive 95/46/CE, en tant qu'instrument de droit dérivé visant à assurer la protection des droits fondamentaux, expliquera l'interprétation dont elle a pu faire l'objet par la Cour de justice des Communautés européennes. Celle-ci a confirmé que ses dispositions doivent être interprétées à la lumière de la protection de la vie privée qu'offre l'article 8 de la Convention européenne des droits de l'homme. Conformément à l'invocabilité dont bénéficient

habituellement les directives vis-à-vis des autorités publiques, la Cour a également eu l'occasion de confirmer que la directive peut être invoquée directement par le particulier afin d'écarter l'application des règles de droit interne contraires à ces dispositions, pour autant que celles-ci apparaissent à la fois inconditionnelles et suffisamment précises. Elle s'est prononcée en ce sens dans une affaire où se posait la question de savoir si la transmission au public, par le *Rechnungshof* (Cour des comptes) autrichien, de données relatives aux rémunérations versées par divers organismes publics soumis à son contrôle à des employés, lorsque ces rémunérations dépassent un certain montant, ainsi que du nom des bénéficiaires, respectait bien l'exigence de proportionnalité inscrite à l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme ainsi qu'à l'article 6, paragraphe 1er, *littera* c, de la directive 95/46/CE (selon lequel les données doivent être «*adéquates, pertinentes et non excessives*» au regard des finalités), et à son article 7, *litterae* c et e, qui font figurer parmi les principes de légitimation des données la nécessité pour le responsable du traitement de respecter une obligation légale à laquelle il est soumis ainsi que la nécessité de «*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 sont communiquées*» (CJCE 20 mai 2003, *Österreichischer Rundfunk e.a.*, C-465/00, C-138/01 et C-139/01, *rec.* I 4989, pts 66s.).

**12.** Ce développement est naturellement bienvenu. Il est de nature à compenser partiellement le caractère incomplet ou peu satisfaisant de la transposition dont la directive 95/46/CE a pu faire l'objet dans certains Etats membres. En un sens cependant, il ne fait qu'accentuer la difficulté que peuvent éprouver parfois les Etats membres à réconcilier leur obligation de transposition fidèle de la directive avec leur obligation d'assurer cette transposition dans le respect des autres droits fondamentaux qui figurent parmi les principes généraux du droit de l'Union et, à présent, dans la Constitution européenne. L'arrêt *Lindqvist* rendu le 6 novembre 2003 par la Cour de justice des Communautés européennes est à cet égard exemplaire (CJCE 6 novembre 2003, *Lindqvist*, C-101/01, *Nep*). Comme Mme Lindqvist, condamnée pour n'avoir pas respecté la loi suédoise relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, prétendait que la



directive 95/46/CE pourrait être illégale au regard de la liberté d'expression, dès lors qu'elle ne définit pas elle-même où situer l'équilibre entre la vie privée, d'une part, la liberté d'expression, d'autre part, la Cour répond que les dispositions de la directive 95/46/CE «*sont nécessairement relativement générales vu qu'elle doit s'appliquer à un grand nombre de situations très diverses* (...) *c'est donc à juste titre que cette directive comporte des règles caractérisées par une certaine souplesse et qu'elle laisse dans de nombreux cas aux États membres le soin d'arrêter les détails ou de choisir parmi des options*» (pt 83), pour en déduire que «(s'il) *est vrai que les États membres disposent à maints égards d'une marge de manoeuvre en vue de la transposition de la directive 95/46* (...) *rien ne permet de considérer que le régime que celle-ci prévoit manque de prévisibilité ou que ses dispositions sont, en tant que telles, contraires aux principes généraux du droit communautaire et, notamment, aux droits fondamentaux protégés par l'ordre juridique communautaire*» (pt 84). Il n'en demeure pas moins que la directive laisse subsister au bénéfice des Etats membres une marge d'appréciation importante, qu'ils doivent utiliser dans le respect des autres droits fondamentaux – notamment la liberté d'expression –, mais sans pour autant priver la directive de la protection qu'elle accorde à la vie privée à l'égard des traitements de données à caractère personnel : l'équilibre voulu par le législateur communautaire ne sera pas toujours aisé à identifier.

### B. – *Les principes de la directive 95/46/CE*

**13.** Comme la Convention n° 108 du Conseil de l'Europe, la directive 95/46/CE vise à préserver l'individu des risques que comporte le traitement de données à caractère personnel qui le concernent en lui offrant des garanties d'ordre, à la fois, substantiel et procédural. L'article II-68, paragraphe 2, de la Constitution européenne offre un résumé de ces garanties, dont il faut aller rechercher l'explicitation dans le texte de la directive. Les garanties substantielles consistent à imposer au responsable du traitement qu'il traite ces données à caractère personnel loyalement et licitement, qu'il ne collecte ces données qu'à des fins déterminées, explicites et légitimes, et ne les traite pas ultérieurement de manière incompatible avec ces finalités. Afin d'éviter un traitement indiscriminé de données à caractère personnel, la directive impose que les données traitées soient adéqua-

tes, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, et qu'elles soient 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; c'est la traduction que reçoit, dans le domaine spécifique de la protection de l'individu à l'égard du traitement des données à caractère personnel, le principe selon lequel toute ingérence dans la vie privée doit respecter une exigence de proportionnalité. La directive exige également que les données traitées soient exactes et, si nécessaire, mises à jour (l'ensemble des règles qui vient d'être énuméré figure à l'article 6 de la directive, relatif aux principes relatifs à la qualité des données).

**14.** La directive 95/46/CE énumère limitativement les fins que peut légitimement vouloir poursuivre le traitement de données à caractère personnel. Parmi les fins reconnues comme légitimes (la liste complète figure à l'article 7 de la directive qui énonce les principes relatifs à la légitimation des traitements de données) figurent, notamment, l'hypothèse où la personne concernée a indubitablement donné son consentement, celle où le traitement 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, ou encore celle où le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis. Bien que la légitimation du traitement par le consentement de la personne concernée puisse apparaître problématique, notamment dans le cadre des rapports d'emploi, les difficultés d'interprétation seront encore plus importantes à propos d'une autre hypothèse de légitimation que retient la directive, celle où le traitement est «*nécessaire à la réalisation de l'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*» (un droit d'opposition est cependant reconnu à la personne concernée à l'article 14 de la directive). Le traitement des données dites «sensibles», qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle, ne sont autorisés que dans des cas limitativement énumérés, et moyennant des garanties particulières (art. 8 de la directive).



**15.** Ces garanties substantielles sont complétées par des garanties procédurales qui visent à assurer leur respect effectif. La personne concernée par le traitement doit être informée de celui-ci (art. 10 et 11 de la directive 95/46/CE). Elle se voit reconnaître un droit d'accès et de rectification, c'est-à-dire le droit d'obtenir du responsable du traitement la communication, sous une forme intelligible, des données faisant l'objet des traitements, et si ces données s'avèrent incomplètes ou inexactes ou le traitement illégal pour d'autres motifs, la rectification ou l'effacement de ces données, ou leur verrouillage (art. 12). La personne concernée peut encore, sous certaines conditions, exercer un droit d'opposition, c'est-à-dire s'opposer au traitement des données à caractère personnel qui la concernent (art. 14); et elle est placée à l'abri de l'adoption à son égard de décisions individuelles automatisées (art. 15). Enfin, le responsable du traitement doit garantir la confidentialité des données ainsi que leur sécurité afin de protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés (art. 16 et 17).

**16.** Ainsi que l'illustre déjà le principe de la légitimation des données qu'elle affirme – c'est-à-dire le principe selon lequel le traitement de données personnelles n'est admis que si celui-ci poursuit une fin reconnue comme légitime –, la directive 95/46/CE fixe le seuil de protection de la vie privée à l'égard des traitements de données à caractère personnel dans l'ensemble des Etats membres à un niveau qui, à plusieurs égards, apparaît plus élevé que celui défini dans la Convention n° 108 du Conseil de l'Europe, dont elle entend par conséquent «*préciser et amplifier*» les principes (préambule, cons. 11).

Trois avancées importantes sont encore à relever plus particulièrement. Premièrement, la directive ne porte pas exclusivement sur les traitements «*automatisés*», auxquels se limite la Convention du Conseil de l'Europe *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*. Elle s'applique au contraire à tout «*traitement*» d'une donnée à caractère personnel, qu'il s'agisse ou non d'un traitement «*automatisé*», pourvu seulement que le traitement non automatisé porte sur des données à caractère personnel contenues ou appelées à figurer dans un fichier

(art. 3, §1, de la directive). La définition du «*traitement*» que fournit l'article 2, *litt.* b, de la directive est particulièrement large : «*toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction*». Ainsi, non seulement cette dernière énumération n'est qu'exemplative, mais en outre elle fait figurer la simple «*collecte*» de données parmi les «*traitements*» auxquels elle s'applique; cela implique, par exemple, que le fait de filmer des personnes, même sans conservation des images – par exemple afin d'assurer à distance la surveillance d'un lieu déterminé – doit respecter les dispositions de la directive.

**17.** Deuxièmement, la directive 95/46/CE du 24 octobre 1995 prévoit que chaque Etat membre doit mettre sur pied une autorité de contrôle indépendante. L'article II-68, paragraphe 3, de la Constitution européenne doit s'interpréter en tenant compte des exigences que formule à cet égard la directive : l'autorité de contrôle doit disposer de pouvoirs d'investigation, y compris du pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle, et de pouvoirs effectifs d'intervention, «*tels que, par exemple, celui de rendre des avis préalablement à la mise en oeuvre des traitements, (...), et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques*». L'autorité de contrôle doit encore pouvoir «*ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire*» (art. 28 de la directive; les pouvoirs qui doivent être reconnus à l'autorité de contrôle installée dans chaque Etat membre sont définis à l'art. 28, §3). Ce point est d'importance capitale, car, dans bien des cas, compte tenu de la nature même de la violation de son droit au respect de la vie privée dont il est victime, l'individu demeurera dans



l'ignorance de celle-ci; et même s'il a connaissance du développement de certaines pratiques ou de l'adoption de certaines réglementations qui lui paraissent incompatibles avec le respect dû à la vie privée dans le traitement des données à caractère personnel, il hésitera à en solliciter le contrôle, par crainte de s'exposer ou en raison du caractère diffus de la violation. Il est donc essentiel, pour une protection effective du droit au respect de la vie privée à l'égard des traitements de données à caractère personnel, qu'une autorité de contrôle puisse assurer une mission de surveillance du respect de la législation en vigueur : la vigilance des individus concernés ne suffit pas, dans la plupart des cas, à ce que les éventuels abus soient sanctionnés. Dans le cadre du Conseil de l'Europe, la Convention n° 108, silencieuse à l'origine sur cette question, ne sera complétée qu'en 2001 par un *Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontaliers de données*.

**18.** Troisièmement, la directive 95/46/CE du 24 octobre 1995 prévoit des règles spécifiques relatives à la transmission vers des Etats tiers de données à caractère personnel (sur ce point également, la Convention n° 108 du 28 janvier 1981 sera complétée par le Protocole additionnel du 8 novembre 2001 *à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontaliers de données*, qui s'inspire étroitement de la directive 95/46/CE). Un tel transfert n'est en principe autorisé que si le pays tiers en question assure un niveau de protection «*adéquat*», le caractère «*adéquat*» du niveau de protection devant s'apprécier «*au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données*». L'article 25 de la directive prévoit la possibilité pour la Commission d'engager des négociations avec les pays n'offrant pas, à son avis, un niveau de protection adéquat, faisant obstacle au transfert vers ces pays de données à caractère personnel, afin d'aboutir à une solution satisfaisante du point de vue du respect des droits fondamentaux de la personne. L'article 26 prévoit en outre un certain nombre d'exceptions au principe de l'interdiction du transfert de données vers un pays, à défaut de niveau de protection adéquat.

**19.** Ces dispositions ont donné lieu, le 24 juillet 1998, à une prise de position du Groupe de travail «*protection des données*» créé par l'article 29 de la directive 95/46/CE (art. 29 Working Party, Working Document, *Transfers of Personal Data to Third Countries : Applying Articles 25 and 26 of the EU Data Protection Directive*, 24th July 24 1998, WP 12). Elles ont été largement débattues (en doctrine, v. M.V. Perez Asinari et Y. Poullet, «The airline passenger data disclosure case and the EU-US debate», *Computer Law & Security Report*, Vol. 20 n° 2, 2004, p. 98) en 2003-2004, à la suite d'une déclaration commune faite, le 18 février 2003, par la Commission européenne et les autorités compétentes des Etats-Unis, selon laquelle elles viseraient à identifier une solution permettant la transmission des données personnelles relatives aux passagers par les compagnies aériennes opérant des vols transatlantiques, selon le système APIS (*Advance Passenger Information System*). Cette déclaration était faite alors que les autorités des Etats-Unis avaient annoncé leur intention, à partir du 5 mars 2003, d'exiger de la part des compagnies aériennes opérant des vols vers les Etats-Unis la transmission de données à caractère personnel concernant les passagers – en dépit des réserves que peut susciter pareille transmission de données au regard de la directive 95/46/CE et du règlement n° 2299/89 du 24 juillet 1989 (Règlement (CEE) n° 2299/89 du Conseil, du 24 juillet 1989, *instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation*, *JOCE* L 220 du 29 juillet 1989, p. 1, amendé en dernier lieu par le règlement du Conseil n° 323/1999 du 8 février 1999, *JOCE* L 40 du 13 fevrier 1999, p. 1; l'art. 6, *litt.* d, du règlement n° 2299/89 prévoit que «*les informations personnelles concernant un consommateur et émanant d'un agent de voyage ne sont mises à la disposition des parties étrangères à la transaction qu'avec le consentement du consommateur*»). La situation créée par les instruments adoptés par les Etats-Unis à la suite des attentats terroristes du 11 septembre 2001 (*Aviation and Transport Security Act* 2001; *Enhanced Border Security and Visa Entry Reform Act* 2002) avait ainsi placé les compagnies aériennes concernées dans une situation particulièrement incertaine, puisque, si elles acceptaient de donner accès aux informations contenues dans les systèmes de réservation (*Passenger Names Records – PNR*), elles s'exposaient au reproche de ne pas respecter les obligations qui leur sont imposées en vertu des instruments précités; or si elles refusaient cet accès, elles risquaient l'imposition de pénalités financières par les autorités américaines, voire l'interdiction d'atterissage sur le territoire des Etats-Unis.



Au moment de la clôture de ce commentaire, une solution paraît avoir été trouvée. Dans l'intervalle, le Parlement européen (v. notamment le rapport préparé au sein de la commission des libertés et droits des cityens, de la justice et des affaires intérieures du Parlement européen par J. L. A. Boogerd-Quaak, le 7 avril 2004 (doc. PE A5-0271/2004); également, notamment, la question écrite E-3440/02 posée par Marco Cappato (NI) au Conseil, portant sur l'échange de données personnelles entre Europol et les États-Unis, *JOUE* n° C 222 E du 18 septembre 2003, p. 71), le Groupe de travail «Article 29» (avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis, adopté par le groupe de travail le 24 octobre 2002, disponible sur le site : http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/ 2002/wp66_fr.pdf; Avis 4/2003 sur le niveau de protection assuré aux États-Unis pour la transmission de données passagers, adopté par le groupe de travail le 13 juin 2003, disponible sur http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_fr.pdf; Avis 2/2004 sur le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (US CBP), adopté par le groupe de travail le 29 janvier 2004, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/ 2004/wp87_fr.pdf) et le Réseau d'experts indépendants en matière de droits fondamentaux (Réseau UE d'experts indépendants en matière de droits fondamentaux, Observation thématique n° 1 : l'équilibre liberté/sécurité dans les réponses de l'Union européenne et de ses Etats membres à la menace terroriste, mars 2003, pp. 22-24; Rapport sur la situation des droits fondamentaux dans l'Union européenne en 2003, mars 2004, pp. 56-59) ont pris position dans le débat, chaque fois afin de rappeler le niveau des exigences imposées par le droit européen en matière de protection des données à caractère personnel et afin de s'interroger sur le caractère adéquat du niveau de protection offert aux Etats-Unis. A la suite des négociations entamées entre la Commission européenne et les autorités américaines, celles-ci ont pris un

certain nombre d'engagements supplémentaires, conduisant la Commission à adopter une décision (décision de la Commission du 14 mai 2004 *relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis*, *JOUE* L 235 du 6 juillet 2004, p. 11) valable pour une période initiale de trois années et demie déclarant qu'«*aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, le Bureau des douanes et de la protection des frontières des États-Unis est considéré comme assurant un niveau de protection adéquat des données de dossiers passagers transférées depuis la Communauté en ce qui concerne les vols à destination ou au départ des États-Unis, conformément à la déclaration d'engagement* [du Bureau des douanes et de la protection des frontières des États-Unis, annexée à la décision]».

Parallèlement, la Commission propose au Conseil la conclusion d'un accord entre la Communauté européenne et les États-Unis sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure (proposition de décision du Conseil *concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure*, COM(2004)190 final – CNS 2004/0064, du 17 mars 2004). Fondé sur l'article 300, paragraphe 2, du traité CE, l'accord vise à permettre au Bureau des douanes et de la protection des frontières des Etats-Unis d'accéder, par voie électronique, aux données PNR provenant des systèmes de contrôle des réservations et des départs des transporteurs aériens situés sur le territoire des États membres de la Communauté européenne, jusqu'à ce qu'un système satisfaisant soit mis en place pour permettre la transmission de ces données par les transporteurs aériens. Un tel accord permettrait de présenter le transfert de données relatives aux passagers des vols transatlantiques par les opérateurs européens comme «*nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis*», au sens de l'article 7, *litt.* d, de la directive 95/46/CE, assurant ainsi la légitimation du traitement. Une incertitude pèse encore sur la compatibilité des solutions ainsi proposées,



qu'il appartiendra à la Cour de justice des Communautés européennes de trancher.

**20.** Enfin, une quatrième particularité de la directive 95/46/CE réside dans le mécanisme de suivi qu'elle institue. La directive met sur pied un Groupe de travail – dit «*Groupe de travail 'Article 29'*» – de caractère consultatif et indépendant, chargé de contribuer à la mise en oeuvre homogène des instruments communautaires relatifs à la protection des données à caractère personnel (ce groupe de travail a vu ses compétences étendues à la directive 2002/58/CE, par l'effet de l'art. 15, §3 de celle-ci; sur la directive 2002/58/CE, voir *infra*) et de formuler des avis et recommandations à l'intention de la Commission européenne. Ce groupe de travail est composé des représentants délégués par les autorités de contrôle instituées au sein de chaque Etat membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission (art. 29, §2). Parmi les missions que lui attribue l'article 30 de la directive 95/46/CE, figure celle d'informer la Commission, s'il constate l'existence de divergences entre les Etats membres «*susceptibles de porter atteinte à l'équivalence de la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté*» (art. 30, §2). Les avis et recommandations du «Groupe de travail Article 29» sont transmis à la Commission – qui doit indiquer les suites qu'elle y donne – ainsi qu'à un comité composé de représentants des Etats membres mais présidé par un représentant de la Commission. Ce dernier comité, créé par l'article 31 de la directive, est consulté par la Commission sur les projets de celle-ci en matière de protection des données.

**21.** Parmi les mesures de suivi que prévoit la directive 95/46/CE, figure l'établissement par la Commission d'un rapport périodique sur sa mise en oeuvre. Dans le premier rapport d'évaluation présenté en mai 2003 conformément à l'article 33 de la directive 95/46/CE (COM(2003) 265 final, 15 mai 2003; l'article 33 de la directive 95/46/CE du 24 octobre 1995 prévoit que, au plus tard pour le 24 octobre 2001, soit trois années après l'expiration de la date limite fixée pour la transposition par les Etats membres de la directive, la Commission fait rapport au Parlement européen et au Conseil sur son application, en faisant, le cas échéant, des propositions de modification; ce rapport a finalement été publié par la Commission

en mai 2003), la Commission a identifié trois difficultés, reliées entre elles, qui peuvent expliquer dans certains cas, Etats ou secteurs d'activités, un niveau de conformité relativement faible avec les exigences de la protection de la vie privée à l'égard des traitements de données à caractère personnel, selon les principes de cette directive et les mesures nationales qui en assurent la transposition. La Commission note, d'abord, «*un manque de ressources affectées à la mise en oeuvre et des autorités nationales en charge d'un très grand nombre de tâches parmi lesquelles les mesures de mise en application bénéficient d'une priorité relativement basse*»; elle constate aussi «*un respect très inégal par les responsables du traitement, à l'évidence réticents à modifier leurs pratiques actuelles pour respecter des règles qui peuvent paraître complexes et contraignantes, alors que les risques d'être pris paraissent relativement faibles*»; enfin, elle identifie «*un niveau apparemment faible de connaissance de leurs droits par les personnes concernées*».

### C. – *L'extension des garanties de la directive 95/46/CE aux institutions et organes communautaires*

**22.** Introduit dans le traité CE par le traité d'Amsterdam, entré en vigueur le 1er mai 1999, l'article 286 dispose que les actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sont applicables aux institutions et organes communautaires; il prévoit également l'institution d'un organe indépendant de contrôle chargé de surveiller l'application desdits actes communautaires aux institutions et organes communautaires. Le Parlement européen et le Conseil ont adopté, sur cette base, le règlement (CE) n° 45/2001 du 18 décembre 2000 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données* (*JOCE* L 8 du 12 janvier 2001, p. 1).

**23.** Le règlement étend aux institutions et organes communautaires les règles de la directive 95/46/CE, et prévoit notamment, à cet égard, que chaque institution ou organe communautaire désignera une personne comme «*délégué à la protection des données*» qui veillera, de manière indépendante, au respect du règlement et disposera à cet effet du personnel et des ressources nécessaires (art. 24 du règlement n° 45/2001). Il crée également un «*contrôleur européen de la protection des données*», avec lequel les institutions et organes communautaires sont tenues de coopérer; le règlement n° 45/2001 a été mis en oeuvre sur ce point par la décision 1247/2002/CE du Parlement européen, du Conseil et de la Commission du 1er juillet 2002 *relative au statut et aux conditions générales d'exercice des fonctions de contrôleur européen de la protection des données* (*JOCE* L 183 du 12 juillet 2002, p. 1) ainsi que par la décision 2004/55/CE du Parlement européen et du Conseil du 22 décembre 2003 *portant nomination de l'autorité de contrôle indépendante prévue à l'article 286 du traité CE (contrôleur européen de la protection des données)* (*JOCE* L 12 du 17 janvier 2004, p. 47). Celui-ci reçoit la mission d'assurer le contrôle de l'application des dispositions du règlement n° 45/2001 à tous les traitements effectués par une institution ou un organe communautaire. Il pourra prendre appui à cet égard sur le «*délégué à la protection des données*» dont doit se doter chaque institution ou organe de la Communauté. Le contrôleur européen de la protection des données doit notamment contrôler au préalable les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées en raison de la nature des informations traitées (données sensibles) ou des conséquences que le traitement des données peut produire sur les personnes concernées (traitements pouvant conduire à évaluer des personnes ou à la priver du bénéfice d'un droit, d'une prestation ou d'un service), ou encore parce que permettant des interconnexions non prévues en vertu de la législation nationale ou communautaire entre des données traitées pour des finalités différentes (art. 27 du règlement n° 45/2001).



### D. – *Les directives sectorielles*

**24.** La directive 95/46/CE du 24 octobre 1995 prévoyait que les principes énoncés par elle «*pourront être complétés ou précisés, notamment pour certains secteurs, par des règles spécifiques conformes à ces principes*» (préambule, cons. 68). L'ouvrage du législateur européen reste, sur ce plan, inachevé.

**25.** Succédant à la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications* (*JOCE* L 24 du 30 janvier 1998, p. 1), à

laquelle elle vient se substituer afin de tenir compte de l'évolution des marchés et des technologies des services de communications électroniques, la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*, dite «*directive vie privée et communications électroniques*», (*JOCE* L 201 du 31 juillet 2002 p. 37; la date limite de transposition par les Etats membres est fixée au 31 octobre 2003) vise à entourer de certaines garanties le traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté (art. 3, §1er de la directive 2002/58/CE). Une des particularités de la directive 2002/58/CE est, en outre, qu'elle vise à protéger les intérêts légitimes des abonnés aux services de communications électroniques qui sont des personnes morales (art. 1, §2), alors que la directive 95/46/CE ne protège que la vie privée des personnes physiques (art. 1, §1er).

**26.** La directive 2002/58/CE oblige notamment les États membres à garantir dans la législation nationale «*la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée* (...)» (art. 5, §1er; la directive définit les «*données relatives au trafic*» comme «*toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation*», art. 2, al. 2, *litt.* b). Cependant, parmi les questions qui, du point de vue du respect des droits fondamentaux, ont été le plus vivement débattues non seulement au cours de la préparation de la directive mais également par la suite, figure celle de la conservation des données de trafic en vue de faciliter des enquêtes et poursuites pénales.

**27.** L'article 15, paragraphe 1er, de la directive recourt à une formule vague, disant que les Etats peuvent apporter des restrictions



à un ensemble des garanties que prévoit la directive «*lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques* (...)». Cette possibilité de restrictions concerne, notamment, la garantie précitée relative à la protection de la confidentialité des communications, mais également la garantie selon laquelle, sauf certaines exceptions limitativement énumérées (aux art. 6, §§2, 3 et 5, de la directive 2002/58/CE), les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public seront «*effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication*» (art. 6, §1er), plusieurs des garanties entourant l'identification de la ligne appelante et de la ligne connectée (art. 8) et celles entourant les données de localisation autres que les données de trafic (art. 9). L'article 15, paragraphe 1er, prévoit, en particulier, que «*les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe* (...)». Bien que de telles mesures doivent respecter les droits fondamentaux, et notamment l'article 8 de la Convention européenne des droits de l'homme (l'article 15, §1er de la directive précise, *in fine*, que «*Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne*»; cette précision est naturellement redondante puisque, dès lors qu'ils s'incrivent dans le cadre d'une exception que ménage a leur profit de le droit de l'Union, les Etats membres sont tenus au respect des droits fondamentaux figurant parmi les principes généraux du droit de l'Union, indépendamment des obligations découlant pour eux d'autres instruments internationaux de protection des droits de l'homme), des questions subsistent quant au caractère proportionné de la durée de conservation des données de trafic que certains Etats membres souhaitent imposer aux opérateurs de services de télécommunications. Après qu'un projet de

décision-cadre eut été divulgué, prévoyant que les Etats membres de l'Union européenne imposeront aux opérateurs de services de télécommunications la conservation des données de trafic pour une période de 12 mois au moins et de 24 mois au plus, afin de permettre l'accès à ces données aux autorités chargées de vérifier l'application effective de la loi (ceci correspond à une des ambitions affichées par le Conseil de l'Union européenne dans le plan d'action qu'il a adopté à la suite des attentats du 11 septembre, où le Conseil invitait la Commission européenne à faire des propositions «*pour veiller à ce que les autorités répressives aient la possibilité d'enquêter sur des actes criminels comportant l'utilisation de systèmes de communications électroniques et de prendre des mesures contre leurs auteurs*»; Conclusions de la session extraordinaire du Conseil du 20 septembre 2001, pt 4, p. 6, doc. 12019/01, presse 327), les commissaires européens à la protection des données ont exprimé leurs doutes quant à la légitimité et à la légalité de telles mesures. Ils ont exprimé le point de vue selon lequel «*lorsque des données de trafic doivent être conservées, sa nécessité doit être démontrée, la période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou toute autre forme d'abus. La conservation systématique de tout type de données pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable*» (déclaration des Commissaires européens à la protection des données, adoptée lors de la conférence internationale de Cardiff (9-11 septembre 2002), *relative à la conservation systématique et obligatoire des données de trafic des télécommunications*). Le «Groupe de travail Article 29» de protection des données a appuyé cette position, dans un avis 5/2002 qu'il a adopté le 11 octobre 2002 (11818/02/FR/final, WP 64). Il y a lieu, par conséquent, pour les Etats membres d'adopter une approche prudente dans l'interprétation de l'article 15, paragraphe 1er de la directive 2002/58/CE, en particulier en ce qui concerne l'obligation de conservation des données de trafic pendant une période plus ou moins longue (pour des développements sur cette question, v. l'Observation thématique n° 1 du Réseau UE d'experts indépendants en matière de droits fondamentaux, «L'équilibre entre liberté/sécurité dans les réponses de l'Union européenne et de ses Etats membres à la menace terroriste», mars 2003, spec. partie IV.3).



**28.** L'adoption d'une directive sectorielle serait hautement souhaitable également dans le domaine des relations d'emploi, tant ce domaine présente des spécificités par rapport à l'approche générale prise par la directive 95/46/CE du 24 octobre 1995 (en faveur d'une telle directive et pour un examen des garanties qu'elles pourrait contenir, v. O. De Schutter, «La protection du travailleur vis-à-vis des nouvelles technologies dans l'emploi», *RTDH* 2003, p. 627). Les dispositifs techniques d'aide à la décision de l'employeur dans la gestion des personnes qui sont candidates à un emploi ou qui, le contrat de travail étant conclu, se trouvent sous son contrôle ou sa direction, se multiplient. L'on peut y faire figurer, notamment, les tests de personnalité et d'intelligence utilisés dans le recrutement et construits par un logiciel spécifique (V., par ex., les systèmes-experts décrits dans le 9ème rapport d'activité de la Commission nationale informatique et libertés (CNIL) pour 1988, p. 179), l'enregistrement des entretiens d'embauche afin de permettre son évaluation par d'autres personnes que l'interviewer ou de mieux apercevoir les réactions de l'interviewé, les dispositifs de surveillance du travail au sein de l'entreprise (par ex., le recours à la vidéosurveillance ou au comptage et au mesurage du travail par ordinateurs [V. spéc. le rapport de la consultation publique de la CNIL, *La cybersurveillance de salariés dans l'entreprise*, mars 2001]), l'utilisation de badges de sécurité permettant l'identification des membres du personnel mais également leur localisation, à tout moment, au sein de l'entreprise. Il est important qu'une initiative communautaire intervienne rapidement afin d'harmoniser la manière dont les Etats membres réglementent ces pratiques (conformément à l'article 138, §2, TCE, les partenaires sociaux ont été invités à prendre part à une consultation sur la protection des données à caractère personnel des travailleurs, lancée le 27 août 2001; le 31 octobre 2002, a été lancée la deuxième phase de consultation des partenaires sociaux; aucune suite publique n'a encore été donnée à ces consultations). Un cadre législatif harmonisé facilitera le déploiement des activités des sociétés multinationales opérant sur plusieurs Etats membres, notamment dans la gestion de leurs ressources humaines. Surtout, le cadre général de la directive 95/46/CE n'apparaît pas totalement adéquat dans le contexte des rapports d'emploi, que caractérise un déséquilibre entre le travailleur et l'employeur, et peut appeler au bénéfice de celui-là certaines garanties supplémen-

taires, dans le respect des prérogatives de celui-ci et, notamment, de son pouvoir d'organiser le travail au sein de l'entreprise.

**29.** L'apport d'une directive spécifique portant sur le traitement des données personnelles dans le cadre de la relation d'emploi devrait présenter l'avantage de clarifier le régime applicable sur quatre points en particulier (le 13 septembre 2001, le «Groupe de travail Article 29» sur la protection des données, établi en tant qu'organe consultatif européen indépendant par l'article 29 de la directive 95/46/CE précitée, a rendu un avis *sur le traitement des données à caractère personnel dans le contexte professionnel*, dans lequel il identifie les principales difficultés que pose l'application aux rapports d'emploi des principes de la directive 95/46/CE et de la directive 97/66/CE, avis n° 8/2001, WP 48, 5062/01, 13 septembre 2001).

Le premier point porte sur la mise en oeuvre de plans d'action positive au sein de l'entreprise, en vue de favoriser l'intégration de certaines catégories sous-représentées dans certains secteurs ou à certains niveaux de la hiérarchie professionnelle. Pareille démarche suppose le traitement de données qualifiées de «sensibles» dans le droit de la protection de l'individu vis-à-vis du traitement de données à caractère personnel, la caractéristique commune de ces données étant qu'elles sont en principe sans pertinence et que leur utilisation peut déboucher sur des discriminations illégitimes ou arbitraires. Or, en raison de cette suspicion, les données sensibles font l'objet d'une protection particulière : elles devraient en principe ne pas être collectées, ou bien uniquement moyennant certaines garanties spécifiques. Sont désignées comme données «sensibles», outre les données relatives à l'origine ethnique ou «raciale», les données relatives aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, les informations relatives à la santé ou à la vie sexuelle (v. le principe 5 des *Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel*, adoptés par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990; l'article 6 de la Convention n° 108 du Conseil de l'Europe, précitée; ou l'article 8 de la directive 95/46/CE, précitée; ainsi que, notamment, l'article 31 de la loi française du 6 janvier 1978 «Informatique et libertés» ou l'article 6 de la loi belge du 8 décembre 1992. Le principe 10.1. contenu dans la recommandation n° R(89)2 adressée



le 18 janvier 1989 par le Comité des Ministres aux Etats membres du Conseil de l'Europe, qui porte sur la protection des données à caractère personnel utilisées à des fins d'emploi, prévoit que les données sensibles «*ne devraient être collectées et enregistrées que dans des cas particuliers, dans les limites prévues par le droit interne et conformément aux garanties appropriées y figurant. En l'absence de telles garanties, ces données ne devraient être collectées et enregistrées qu'avec le consentement exprès et éclairé des employés*». Sur cet important instrument que constitue la recommandation n° R(89)2 du Comité des Ministres du Conseil de l'Europe, v. P. DE HERT et S. GUTWIRTH). Il peut en résulter, pour l'employeur, une tension entre son obligation de ne pas maintenir des critères, des dispositifs ou des pratiques qui créent un impact disproportionné sur certaines catégories de travailleurs au détriment de leur droit à l'égalité de traitement – la mesure d'un tel impact supposant le traitement de données «sensibles» – et son obligation de se conformer à toutes les garanties qui doivent entourer le traitement de telles données (sur cette tension, v. O. DE SCHUTTER, *Discriminations et marché du travail. Egalité et liberté dans les rapports d'emploi*, Bern-Bruxelles-Oxford-New York-Wien, P.I.E. Peter Lang, 2001, pp. 33-52. V. aussi le point de vue exprimé par la Commission européenne dans son document préparatoire à la *Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs*, en vue de définir l'orientation possible d'une initiative communautaire dans ce domaine, p. 14; d'après elle, «*Les données à caractère personnel concernant* (...) *les origines raciales ou ethniques et les convictions religieuses et autres peuvent faire l'objet d'un traitement lorsque la loi autorise un traitement différent, sur la base de l'un de ces motifs, notamment en cas d'exigences professionnelles spécifiques ou d'action positive*»).

Une deuxième question concerne la légitimation du traitement de données à caractère personnel par le consentement de la personne concernée. Pareil mode de légitimation est problématique dans le contexte du rapport d'emploi, compte tenu des conditions qui entourent les rapports de négociation entre le travailleur et l'employeur.

Troisièmement, il y a lieu de faire une place particulière aux partenaires sociaux dans la mise en oeuvre au sein de l'entreprise d'un système de traitement des données à caractère personnel. Selon la

Recommandation n° R(89)2 (*op. cit.*), «*les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction ou à la modification de systèmes automatisés pour la collecte et l'utilisation de données à caractère personnel concernant les employés. Ce principe s'applique également à l'introduction ou à la modification de procédés techniques destinés à contrôler les mouvements ou la productivité des employés*» (principe 3.1.). D'après la CNIL française, le principe de la discussion collective «*donne sa substance au principe de proportionnalité*» (CNIL, rapport sur *La cybersurveillance des salariés dans l'entreprise*, précité, p. 18); son objectif doit être en effet – en vue de limiter au minimum nécessaire l'ingérence dans la vie privée des salariés qui peut résulter par exemple de l'introduction dans l'entreprise d'un nouveau dispositif de contrôle – de rechercher, par la délibération, des solutions alternatives susceptibles de réaliser le même objectif en causant des immixtions moindres dans la vie privée.

**30.** Enfin, il y aurait lieu de clarifier la portée, dans le contexte du processus de recrutement, de l'interdiction des décisions individuelles automatisées. Parmi les dangers qui sont le plus spontanément associés au déploiement des nouvelles technologies de traitement de l'information, notamment des données à caractère personnel, figure celui d'une substitution de la machine à l'humain, pour l'adoption de décisions qui, en raison de l'importance de leurs conséquences pour l'individu, ne peuvent se réduire à une équation à partir de quelques données informatisées. L'article 15 de la directive 95/46/CE prévoit dès lors le droit de toute personne à «*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.*» (V. également sur ce point la recommandation n° 1/2000 sur les données d'évaluation des employés, adoptée par le «Groupe de travail Article 29» sur la protection des données le 22 mars 2000, WP 42, 5008/01). Mais la même disposition prévoit qu'une décision individuelle automatisée est acceptable, notamment, si elle est prise «*dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la*



*possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime*» (art. 15, §2). Il serait souhaitable de confirmer que l'exception qui vient d'être citée ne peut légitimer une automatisation du traitement de données nominatives à des fins de recrutement (cette question n'est pas abordée par le «Groupe de travail Article 29» sur la protection des données dans son avis n° 8/2001 du 13 septembre 2001), d'abord en raison du caractère suspect de tout consentement donné par le travailleur au traitement de données à caractère personnel à ce moment de la relation d'emploi – or c'est, implicitement, sur ce consentement que se fonde l'exception précitée -, mais aussi parce que, par définition, dans la phase du recrutement, la demande de conclusion du contrat n'a pas encore été satisfaite, mais au contraire dépendra des résultats de la sélection opérée par l'employeur.

**31.** Sur un autre plan également, le travail du législateur européen reste inachevé. Ni la directive 95/46/CE, ni la directive 2002/58/CE – qui ont l'une et l'autre pour base juridique l'article 95 du traité CE – ne s'appliquent dans les matières qui relèvent des titres V et VI du traité sur l'Union européenne (politique étrangère et de sécurité commune et coopération judiciaire pénale et coopération policière). En outre, elles ne s'appliquent pas aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal (art. 3, §2, de la directive 95/46/CE; art. 1, §3, de la directive 2002/58/CE). Certes, dans divers instruments adoptés dans le cadre de ce qu'il est convenu d'appeler le «troisième pilier» – recouvrant à la fois les domaines de l'asile et de l'immigration et ceux de la coopération policière et de la coopération judiciaire en matière pénale –, figurent des clauses spécifiques relatives à la protection des données. Un titre entier (titre IV) de la Convention portant création d'un Office européen de police (convention Europol) est ainsi consacré à la protection des données à caractère personnel (la convention Europol a d'abord été adoptée par un acte du Conseil, du 26 juillet 1995, *portant établissement de la convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un Office européen de police* [convention Europol], *JOCE* C 316 du 27 novembre 1995, p. 1; elle a été modifiée à de nombreuses reprises depuis, en dernier lieu par un acte du Conseil du 27

novembre 2003, *JOUE* C 2 du 6 janvier 2004, p. 1. L'article 18 de la convention Europol, concernant la transmission des données à des Etats tiers, a été complété par un acte du Conseil du 12 mars 1999 *arrêtant les règles relatives à la transmission de données à caractère personnel par Europol à des États et des instances tiers*, *JOCE* C 88 du 30 mars 1999, p. 1, ensuite modifié par un acte du Conseil du 28 février 2002 *portant modification de l'acte du Conseil du 12 mars 1999 arrêtant les règles relatives à la transmission de données à caractère personnel par Europol à des États et des instances tierces*, *JOCE* C 058 du 5 mars 2002, p. 12, afin de définir les conditions dans lesquelles les instances tierces auxquelles Europol aura transmis des données pourront en opérer le transfert ultérieur; ce dernier acte n'est cependant plus en vigueur).

La mise en vigueur de la Charte des droits fondamentaux de l'Union qui résultera de la ratification de la Constitution européenne impliquera que, dans toutes les activités des institutions de l'Union, de ses organes ou de ses agences, et quel que soit le domaine matériel des activités concernées, les principes fixés à l'article II-68 de la Constitution européenne devront être respectés. De la même façon que le règlement n° 45/2001 a étendu aux institutions et organes de la Communauté européenne les règles de la directive 95/46/CE, il faut considérer qu'il en résultera l'extension des principes de cette directive à toutes les activités des institutions, organes et agences de l'Union, y compris dans les secteurs excédant le champ d'applicabilité de la directive 95/46/CE. Ceci ne dispense pas de la nécessité de préciser les conséquences qui en découlent dans les domaines de la coopération policière et de la justice pénale; au contraire, cette tâche n'en apparaît à certains égards que plus urgente, dès lors qu'elle sera de nature à faciliter le travail d'interprétation du juge européen.