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

juin 1997
n°40 - 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 DONNEES À CARACTÈRE PERSONNEL EN DROIT COMMUNAUTAIRE[1]

I. – LE CONTEXTE GÉNÉRAL

1. – Le 24 octobre 1995, la Communauté européenne s'est dotée d'une directive générale concernant la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données[2].

Ce texte est l'aboutissement d'un long processus de réflexion et de recherche de consensus entre les différents États membres. C'est que la plupart de ceux-ci, conformément aux obligations contractées au sein du Conseil de l'Europe par la signature de la Convention n° 108[3], disposaient déjà d'une législation nationale ayant un objet similaire.

Si les principes de base de la protection sont analogues, les législations nationales présentent à l'heure actuelle de larges divergences susceptibles de freiner la libre circulation des informations dans le grand marché européen. En outre, l'internationalisation croissante des flux d'informations forçait une réflexion quant aux transferts de données vers les pays tiers[4]. Il fallait enfin tenter de mettre à jour ces législations en tenant compte des leçons tirées de nombreuses années d'application de la Convention n° 108.

2. – Cette convention n'est du reste plus aujourd'hui le seul instrument international régissant tout ou partie de la protection des données à caractère personnel en Europe. L'Union européenne elle-même a adopté, ou est en passe de le faire, divers textes protecteurs dans le cadre soit de sa politique économique (la future directive RNIS[5], le règlement statistique[6], etc.) soit du troisième pilier – coopération dans les domaines de la justice et des affaires intérieures – (Convention Europol[7], future Convention Eurodac[8], etc.). D'autres textes sont issus de sources plus diverses: les nombreuses recommandations sectorielles du Conseil de l'Europe[9] mais aussi les dispositions de la Convention européenne des droits de l'homme susceptibles de

(1) Le présent article ne reflète que l'opinion personnelle de ses auteurs.
(2) Directive 95/46/C.E. 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 des données, *J.O.C.E.*, n° L 281/31, du 23 novembre 1995 (ci-après dénommée «la directive»).
(3) Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel du 28 janvier 1981, Série des traités européens, n° 108 (ci-après «la Convention n° 108»). En principe, cette convention est dépourvue d'effets directs dans l'ordre juridique interne (voy. notamment point 20 du *Rapport explicatif de la Convention*, Conseil de l'Europe, Strasbourg, 1981). Toutefois, certains pays, comme la France, ont reconnu un tel effet à certains de ses articles.
(4) La Convention n° 108 ne contient aucune disposition à cet égard.
(5) Proposition de directive du Parlement européenne et du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications, en particulier des réseaux numériques à intégration de service (RNIS) et des réseaux mobiles numériques, *J.O.C.E.*, n° C 315, du 24 octobre 1996.
(6) Règlement n° 322/97 du Conseil, du 17 février, relatif à la statistique communautaire, *J.O.C.E.*, n° L 52/1, du 22 février 1997.
(7) Convention basée sur l'article K 3 du traité sur l'Union européenne portant création d'un office européen de police (convention Europol) *J.O.C.E.*, n° C 316/2, du 27 novembre 1995.
(8) Projet de Convention Eurodac, pour la collection, le stockage, l'échange et la comparaison des empreintes digitales des demandeurs d'asile.
(9) Recommandations pour la protection des données utilisées à des fins de marketing (R (85) 20 du 25 octobre 1985), de sécurité sociale (R (86) 1 du 23 janvier 1986), dans le secteur de la police (R (87) 15 du 15 septembre 1987, à des fins d'emploi (R (89) 2 du 18 janvier 1989), à des fins de paiement (R (90) 19 du 13 septembre 1990), sur la communication à des tierces personnes des données à caractère personnel détenues par des organismes publics (R (91) 10 du 9 septembre 1991), relative à l'utilisation de l'ADN dans le cadre de la justice pénale (R (92) 1 du 10 février 1992), dans le domaine des services de télécommunications (R (95) 4 du 7 février 1995); pour la protection des données médicales (R (97) 5 du 14 février 1997). Certains textes plus anciens dans les domaines des assurances et de la recherche scientifique et statis

SOMMAIRE

Avis aux auteurs

La rédaction accueille avec plaisir les propositions d'articles qui lui sont soumises. Un document relatif à la notation de références dans le *J.T.D.E.* peut être obtenu sur demande auprès des membres de la rédaction.

s'appliquer[10], les lignes directrices de l'O.C.D.E.[11], la Convention d'Application de Schengen[12], etc.

L'existence de cette multiplicité de textes, parfois juridiquement contraignants, ne sera pas sans poser des problèmes aigus de légistique aux États membres qui doivent conformer à la directive leur législation nationale pour le 24 octobre 1998[13] tout en évitant d'enfreindre les dispositions issues d'autres instruments.

3. – La filiation entre la directive et les textes issus du Conseil de l'Europe est évidente et explicite. Le considérant 10 de la directive indique ainsi que «l'objet des législations nationales relatives au traitement de données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 C.E.D.H. et dans les principes généraux de droit communautaire». Le considérant 11 énonce, quant à lui, que «les principes de protection des droits et libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la Convention du 28 janvier 1981 du Conseil de l'Europe».

Outre des dispositions largement analogues, la similarité entre la directive et la Convention n° 108 se marque par la poursuite de deux objectifs apparemment identiques, à savoir, d'une part, la protection des libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, à l'égard des traitements de données à caractère personnel[14] et, d'autre part, la libre circulation des données[15].

On pourrait bien sûr s'étonner d'une telle convergence. Ces textes sont en effet issus d'organisations internationales dont les buts premiers paraissent *a priori* aux antipodes les uns des autres: la protection des droits de l'homme et libertés fondamentales pour le Conseil de l'Europe, la réalisation d'un marché unique et la promotion de grandes libertés économiques pour l'Union européenne.

4. – En réalité, le but véritable de la directive est d'éviter que la libre circulation de l'information entre États membres, liberté par essence économique, soit excessivement limitée – au surplus de manière différente au sein de chaque État – au nom de droits et libertés de la personne humaine. Dans la mesure où l'objectif premier de l'Union européenne[16] est la création d'un marché sans frontières internes, assurant la libre circulation des marchandises, personnes, services et capitaux, la libre circulation des données apparaît comme une condition indispensable de la création effective de ce marché[17]. Cette libre circulation exige qu'une protection des droits fondamentaux des personnes concernées par ces données soit assurée sinon de manière uniforme[18], du moins de façon équivalente dans les divers États membres, étant entendu qu'elle s'opère, selon les déclarations des considérants, à un niveau élevé[19].

5. – On peut prévoir qu'à l'avenir, les législations nationales de protection des données deviendront, plus que jamais, le terrain d'une confrontation incessante entre, d'une part, les intérêts économiques et commerciaux de responsables de traitements qui n'auront de cesse de légitimer leurs traitements sur les grandes libertés économiques fondant l'Union européenne, et plus précisément sur l'«équilibre» consacré par les dispositions de la directive commentée, et d'autre part, les intérêts de la personne concernée par les données qui mettra en avant les droits et libertés fondamentales qui lui sont reconnus au sein de chaque État membre sur la base des conventions et autres instruments issus du Conseil de l'Europe. Les oppositions pourront d'ailleurs surgir lors d'applications non spécifiques à la libre circulation de l'information, mais par exemple à la liberté de concurrence[20] ou d'établissement.

C'est d'autant plus vrai que les protagonistes disposeront dans l'avenir de voies juridictionnelles différentes afin de tenter de résoudre les probables conflits. Les responsables des traitements préféreront certainement utiliser la voie des procédures introduites devant la Cour européenne de Luxembourg. Les personnes concernées opteront plutôt pour les procédures propres à la Convention européenne des droits de l'homme devant la Cour de Strasbourg. Même si l'on peut s'attendre à des rapprochements entre l'Union européenne et le Conseil de l'Europe[21], les différences de fondement de l'intervention des organes conjointement compétents risquent de déboucher sur des solutions difficilement conciliables.

Ce tiraillement risque encore d'être exacerbé dès lors qu'une marge de manœuvre appréciable est laissée à chaque État membre dans la mise en vigueur des dispositions protectrices de la directive.

6. – L'article 1, *b*, de la directive énonce que «les États membres ne peuvent restreindre ni

tique sont actuellement réexaminés. On peut encore citer la recommandation R (95) 11 du 11 septembre 1995 relative à la sélection, au traitement, à la présentation et à l'archivage des décisions judiciaires. Ces recommandations ne lient que moralement les États signataires.

(10) Principalement l'article 8 (protection de la vie privée et familiale) et l'article 10 (liberté d'expression) de la Convention européenne des droits de l'homme (ci-après C.E.D.H.). Pour une analyse de l'article 8 C.E.D.H., voy. C. Russo, «Article 8, § 1», in L.E. Pettiti, E. Decaux et P. H. Imbert, *La Convention européenne des droits de l'homme*, Paris, Economica, 1995, p. 305 et ss; E. Coussirat-Coustere, «Article 8, § 2», *idem*. Pour une analyse récente de la jurisprudence relative à l'article 8, voy. R. Ergec, «Examen de jurisprudence (1990 à 1994): la Convention européenne des droits de l'homme», *R.C.J.B.*, 1995, p. 341 et P. Lambert, «Examen de jurisprudence: la Cour européenne des droits de l'homme – 1995», *J.T.*, 1996, p. 36 et s. Pour une jurisprudence appliquant l'article 8 C.E.D.H. à la protection des données voy. Cour eur. D. H., arrêt *Leander* du 26 mars 1987, série A, n° 116, § 48. Voy. aussi Req. n° 8334/78, *X c. Autriche*, Req. n° 1307/ 61, *X c. République fédérale d'Allemagne* et Req. n° 8170/78, citées par P. Kayser, *La protection de la vie privée par le droit*, Paris, Economica, 1995, p. 30. Voy. aussi Cour eur. D. H., arrêt *Klass*, du 6 septembre 1978, série A, n° 28; Cour eur. D. H., arrêt *Malone* du 2 août 1984, série A , n° 82; Cour eur. D.H., arrêt *Kruslin* du 24 avril 1990, série A, n° 176; Cour eur. D. H., arrêt *Huvig* du 24 avril 1990, série A, n°176-B.

(11) Lignes directrices de l'O.C.D.E. régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, Paris, O C.D.E., 1981. Ce texte n'est que moralement contraignant.

(12) Convention d'application de l'Accord de Schengen du 14 juin 1985.

(13) Article 32, § 1, de la directive.

(14) Cfr l'article 1er de la Convention n°108: «Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (protection des données)» et l'article 1§1 de la directive: «Les États membres assurent (...) la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur privée, à l'égard des traitements de données à caractère personnel».

(15) Voy. ci-dessous, pt. 6.

(16) Article 7 du Traité de l'Union européenne 7 février 1992, *J.O.C.E.*, 1992, C 231, du 29 juillet 1992.

(17) Voy. le considérant 3 de la directive. La Convention n° 108 poursuit le même objectif de libre circulation des données. C'est toutefois au nom de l'article 10 de la C.E.D.H. (liberté d'expression) que cet objectif doit être réalisé. Le rapport explicatif est très éclairant à cet égard: «Le point de départ de la Convention est que certains droits de la personne doivent être protégés au regard de la liberté de circulation de l'information sans considération de frontières, ce dernier principe étant consacré dans les instruments internationaux et européens sur les droits de l'homme (cfr. article 10 de la C.E.D.H.)».

(18) Il s'agit, dira-t-on, conformément au Traité européen de rapprocher les législations.

(19) Le considérant 11 de la directive déclare que la directive «amplifie» les principes de la Convention n° 108.

(20) Des divergences de réglementations nationales relatives aux données sensibles permises – on le verra – par la directive commentée, pourraient ainsi entraîner des distortsions de concurrence entre des entreprises concurrentes opérant à partir de territoires plus «laxistes».

(21) Entre le Conseil de l'Union européenne et le Comité juridique de protection des données du Conseil de l'Europe, il existe un certain rapprochement, d'une part, via la coordination des textes – c'est ainsi que la conformité du texte de la recommandation R(97) 5 sur la protection des données médicales avec la directive a été examinée préalablement son l'adoption –, d'autre part via des négociations en vue de l'adhésion de la Communauté européenne à la Convention n ° 108 (voy. la recommandation de décision du Conseil de l'Union européenne relative à l'ouverture de négociations en vue de l'adhésion des Communautés européennes à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé de données). Dans un document de travail du 17 avril 1997 relatif à cette question, la Commission européenne estime que l'adhésion de la Communauté à la Convention n° 108 aurait pour conséquence d'intégrer celle-ci dans l'ordre juridique communautaire et ceci à un niveau normatif supérieur à la directive). Cette adhésion donnerait cependant compétence à la Cour de justice des Communautés européennes pour connaître du respect de la Convention n° 108. Sur la jurisprudence de la Cour de justice des Communautés européennes considère que l'article 8 de la Convention européenne des droits de l'homme, voy. C.J.C.E., 5 octobre 1994, *X c. Commission*, C 404/92 P, *Rev. trim. dr. h.*, 1995, p. 98, note O. De Schutter).

interdire la libre circulation des données à caractère personnel entre les États membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1»[22].

La première partie du considérant 9 précise à cet égard que «du fait de la protection équivalente résultant du rapprochement des législations nationales, les États membres ne pourront plus faire obstacle à la libre circulation entre eux des données à caractère personnel pour des raisons relatives à la protection des droits et libertés des personnes, notamment du droit à la vie privée»[23].

L'équivalence de protection décrétée par la directive n'abolit pas toute disparité entre législations nationales. Même si le degré de précision de la directive aurait pu le laisser penser, le considérant 9 atténue fortement ce qui, cependant, aurait dû constituer la conséquence logique de sa prémisse. Il affirme en effet que «les États membres disposeront d'une marge de manœuvre qui, dans le contexte de la mise en œuvre de la directive, pourra être utilisée par les partenaires économiques et sociaux; qu'ils pourront donc préciser, dans leur législation nationale, les conditions générales du traitement des données; que, ce faisant, les États membres s'efforceront d'améliorer la protection assurée actuellement par leur législation; que dans les limites de cette marge de manœuvre et conformément au droit communautaire, des disparités pourront se produire dans la mise en œuvre de la directive»[24].

7. – Certaines dispositions de la directive reconnaissent explicitement la marge de manœuvre. En particulier à propos des flux intraeuropéens, le responsable établi sur plusieurs territoires veillera, selon l'article 4, à assurer le «respect par chacun des établissements des obligations prévues par le droit national applicable». À propos des flux vers les pays tiers, selon l'article 25, c'est d'abord au regard des dispositions nationales prises en application des autres dispositions de la directive que s'opérera l'examen des flux. Plus fondamentalement, c'est à propos des principes fondamentaux de la protection des données que le considérant 22 souligne que «les États membres préciseront dans leur législation ou lors de leur mise en œuvre des dispositions prises en application de la présente directive les conditions générales dans lesquelles le traitement de données est licite; qu'en particulier, l'article 5, en liaison avec les articles 7 et 8, permet aux États membres de prévoir, indépendamment des règles générales, des conditions particulières pour les traitements de données dans des secteurs spécifiques».

Nombreuses sont du reste les dispositions explicites du texte où la plus grande liberté d'interprétation est laissée aux États membres même si elles visent parfois des éléments essentiels de la protection:
- la nécessité de l'exécution d'une mission d'intérêt public (art. 7, *e*), de nature à légitimer certains traitements, pourra être soumise à un contrôle particulier de l'autorité de contrôle ou exiger un fondement légal, selon les principes constitutionnels de chaque pays;
- à propos des données sensibles, l'article 8, § 2, *a*, autorise chaque État à limiter la portée du consentement de la personne concernée dans tous ou certains traitements portant sur de telles données, l'article 8, § 2, *b*, laisse à la législation nationale le soin de définir les traitements de données sensibles justifiés par le respect des obligations et droits nés des législations de droit du travail ainsi que les garanties adéquates entourant de tels traitements, l'article 8, § 4, permet à l'État de légitimer pour des motifs d'intérêt public comportant des traitements de données sensibles au-delà des cas prévus par le reste de l'article 8, enfin, l'article 8, § 7, laisse aux États membres le soin de régler la question des numéros d'identification, nationaux ou de portée générale;
- l'article 9 confère aux États membres le soin de réglementer le secteur de la presse;
- l'article 11 relatif à l'information des personnes concernées lorsque les données n'ont pas été collectées auprès de la personne concernée contient une alternative importante quant au moment de cette information et des possibilités de dérogations importantes, dont chaque État pourra se prévaloir ou non;
- l'article 13 permet à chaque État de limiter certains droits prévus par la directive lorsqu'une limitation est nécessaire pour la sauvegarde d'intérêts publics importants, voire de la protection de la personne concernée ou des droits et libertés d'autrui[25];
- le droit d'opposition prévu à l'article 14 peut être limité par le droit national et l'article 15 autorise pareillement une législation nationale à légitimer les décisions individuelles fondées exclusivement sur un traitement automatisé;
- dans le domaine des obligations administratives de notification à l'autorité de contrôle ou de contrôle préalable, les articles 18, 19, 20 et 21 laissent aux États membres de nombreuses latitudes qui peuvent conduire à des régimes profondément différents qui pourraient influer sur le choix des entreprises à localiser leurs traitements dans tel ou tel État;

- l'article 24 laisse aux États membres le soin de définir les mesures d'application de la directive et en particulier les sanctions de la violation des dispositions prises en application de celle-ci.

8. – Si les auteurs de la directive paraissent avoir été conscients de l'importante marge de manœuvre laissée aux États membres nonobstant le rapprochement des législations opéré par la directive, ils ont en même temps mis en place les instruments d'une nécessaire mais progressive convergence.

On peut ainsi noter à ce propos que:

- en matière de flux transfrontières vers les pays tiers, la politique nationale trouve ses limites dans l'obligation d'informer la Commission tant des autorisations que des refus, ce qui permet à la Commission, avec l'aide du Comité des représentants des États membres de définir une politique commune en la matière;

- la constatation de «divergences susceptibles de porter atteinte à l'équivalence des niveaux de protection» fait l'objet d'un suivi par le «Groupe de protection des personnes», composé de représentants des autorités de contrôle. Ce groupe peut également proposer des interprétations communes du texte de la directive;

- un mécanisme puissant de convergence est constitué par la mise sur pied de codes de conduite communautaires qui échappent à l'examen des autorités nationales de protection des données;

- la prohibition pour des raisons relatives à la protection des données, des restrictions ou interdictions des flux de données à l'intérieur de l'Union européenne, représente une incitation forte pour les pays à ne pas exiger des protections nationales sensiblement plus fortes, protections dont l'efficacité pourrait facilement être détournées par un flux interne à l'Union européenne.

Ainsi, si on doit parler de liberté relative des États membres, cette liberté apparaît surveillée, à défaut d'être contrôlée.

9. – Le présent commentaire suivra largement le plan des dispositions de la directive[26], même si le champ d'application territorial de celle-ci sera étudié, pour des raisons de meilleure compréhension, dans la partie relative aux flux transfrontières de données.

On s'attachera dans un premier temps aux définitions (2), ce qui permettra de mesurer au mieux le champ d'application matériel de la

(22) L'article 12, § 2, de la Convention n° 108 stipule qu'«une partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre Partie».
(23) De manière similaire, le paragraphe 20 du Rapport explicatif de la Convention n° 108 précise qu'«en s'engageant à appliquer ces principes (de la Convention n° 108), les Parties contractantes tendent à supprimer entre elles les restrictions aux flux transfrontières de données, évitant ainsi que le principe de la libre circulation des informations soit mis en cause par des formes de protectionnisme».
(24) L'article 12, *§3, a*, de la Convention n° 108 donne également aux États signataires une certaine marge de manœuvre dans la mesure où il les autorise à prévoir une réglementation spécifique pour certaines catégories de données pour autant que l'autre partie n'apporte pas un niveau de protection équivalent à celles-ci.

(25) L'article 9, *a* et *b*, de la Convention n° 108 contient une disposition identique, à savoir qu'il «est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique:
a. à la protection de la sécurité de l'État, à la sûreté de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales;
b. à la protection de la personne concernée et des droits et libertés d'autrui».

(26) Bien que procédant d'une logique similaire, la structure de la directive n'est pas totalement identique à celle de la Convention n° 108: elle y ajoute de nouveaux chapitres; elle regroupe certaines dispositions de manière différente. L'objet des chapitres un et deux de la directive et de la Convention n° 108 est identique. Le chapitre trois de la directive porte sur la responsabilité, les re-

directive (3). On s'attardera ensuite sur les lignes directrices de la protection (4) et sur l'étude des régimes spécifiques à certaines catégories de traitements (5). Les droits de la personne concernée retiendront alors l'attention ainsi que certaines obligations spécifiques du responsable du traitement (6). Le régime spécifique des flux transfrontières de données fera l'objet d'une large analyse en distinguant les flux intracommunautaires, en ce compris le champ d'application territorial, et ceux poursuivis vers des pays tiers (7). On terminera par un bref commentaire des dispositions relatives à l'utilisation des code de conduite (8), à l'institution d'organes de contrôle et d'interprétation (9) et aux responsabilités (10).

II. DÉFINITIONS

10. – Les réglementations relatives à la protection des données doivent être, autant que possible, indépendantes des évolutions incessantes des technologies de l'information. C'est pourquoi – et la directive commentée ne fait pas exception – leur champ d'application matériel est déterminé au moyen de concepts juridiques abstraits prédéfinis (traitements, données à caractère personnel, etc.). Ces définitions permettent l'insertion des dernières évolutions technologiques dans le champ des réglementations même si le contenu des règles doit, selon les cas, être adapté.

C'est ainsi que la directive européenne s'appliquera, non seulement aux banques de données classiques contenant de l'information personnelle, mais également à des techniques plus évoluées de collectes d'informations (systèmes d'enregistrements d'images numérisées, call centers automatisés, etc.) ou de transmissions d'informations (réseaux mondiaux du type d'Internet, systèmes E.D.I. etc.).

En outre, afin de déterminer au mieux les responsabilités quant aux règles de comportement édictées, d'autres définitions sont également arrêtées: responsable du traitement, sous-traitant, etc.

A. – Les données à caractère personnel

11. – Selon l'article 2, *a*, de la directive, est considérée comme donnée à caractère personnel, «toute information concernant une personne physique identifiée ou identifiable (personne concernée); 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[27]».

La notion d'information n'est pas définie. Dès lors, elle n'est soumise à aucune exigence de forme particulière. Une information écrite, chiffrée, mais celle également présente dans une image ou un son sont constitutives de données[28].

L'information est relative à une personne physique[29]. La directive reste donc fidèle à l'exclusion des personnes morales du champ d'application de la protection[30]. Elle est par contre muette sur son éventuelle application aux données relatives à des personnes physiques décédées[31].

12. – La personne physique doit être «identifiée ou identifiable»[32]. Elle est réputée identifiable dès lors qu'une possibilité existe de l'identifier directement ou indirectement notamment par un numéro de téléphone, de plaque d'immatriculation de voiture, de sécurité sociale ou de passeport. Le texte précise par ailleurs qu'une personne peut être identifiée par référence à un ou plusieurs éléments spécifiques propres à son identité sous toute ses formes (âge, fonction professionnelle, adresse, etc.). Le but paraît ici de viser une identification issue de croisements de caractéristiques propres à certains groupes d'individus.

Se pose alors la question des données anonymes. Dans sa première version, le texte ex-

cours et les sanctions, alors que la Convention n° 108 ne traite pas ces questions dans un chapitre spécifique, mais les aborde dans le chapitre deux, qui contient l'ensemble des principes à la base de la protection. Le chapitre quatre de la directive, intitulé, à l'instar du chapitre quatre de la Convention n° 108 «Flux transfrontières de données» a en réalité un objet différent. Le chapitre quatre de la Convention n° 108 envisage la question des flux transfrontières entre pays liés par cette Convention, tandis que le chapitre quatre de la directive règle les flux transfrontières vers les États non liés par la directive. Le chapitre cinq de la directive relatif aux codes de conduite ne trouve pas d'équivalent dans la Convention n° 108. Enfin, le chapitre six de la directive concernant les autorités nationales de contrôle et le groupe communautaire de protection des données regroupe des dispositions contenues dans les chapitres deux et quatre de la Convention n° 108.

(27) Dans la Convention n° 108, la donnée à caractère personnel signifie «toute information concernant une personne identifiée ou identifiable (personne concernée)».

(28) Voy. le considérant 14 de la directive. Le considérant 16 ajoute que la directive ne s'applique pas aux sons et images s'ils relèvent de traitements poursuivant des fins de sécurité publique, de défense, de sûreté de l'État et de droit pénal. Le considérant 17 précise que la protection sera limitée dans l'hypothèse de traitement de sons et images à des fins de journalisme ou d'expression littéraire ou artistique. Pourtant, aucun régime spécifique n'est prévu par le texte de la directive. La limitation à la protection nécesaire à l'exercice de la liberté d'expression et à la poursuite des fins de sécurité publique sont communes à l'ensemble des données quelle que soit leur nature. L'unique article qui mentionne explicitement les sons et images est l'article 33, § 2, qui prévoit que la Commission examine en particulier l'application de la directive aux traitements de données constituées par des sons et images, relatives aux personnes physiques. Pour une analyse de l'application de la directive à la vidéosurveillance, voy. P. De Hert, O. De Schutter et S. Gutwirth, «Pour une réglementation de la vidéosurveillance», *J.T.*, 1996, pp. 575 et 576. Concernant l'application de la Convention n° 108 aux sons et images, le Comité consultatif institué par cette Convention a considéré que les images et les voix numériques peuvent être assimilées à des données à caractère personnel (voy. T-PD(94)7, Strasbourg, Conseil de l'Europe, 1994, p. 4).

(29) L'article 3, §2, de la Convention n° 108 atorise quant à lui les États signataires à appliquer la Convention aux groupements de personnes physiques jouissant ou non de la personnalité juridique. Il en va de même pour le projet de recommandation du Conseil de l'Europe relative à la protection des données à caractère personnel collectées et traitées à des fins de statistiques. Le paragraphe 64 de l'annexe à la recommandation explique qu'il n'existe pas de conception objective des données personnelles relatives à des groupes humains. Si des données de groupe de personnes ayant un statut juridique (tels le couple ou la famille) sont aisément considérées comme des données à caractère personnel, il n'en va pas de même lorsque les données de groupe relèvent d'agrégation plus large (tels les habitants d'un pâté de maison) (voy. CJ-PD(97)20, p. 40).

(30) Il arrive néanmoins que le traitement de données relatives à des personnes morales révèlent des données personnelles. La Cour européenne des droits de l'homme a jugé de la sorte que la protection offerte par l'article 8 continue à jouer en faveur d'un individu dont les activités professionnelles et non professionnelles s'imbriquent à un point tel qu'il n'existe aucun moyen de les dissocier (pour les écoutes téléphoniques, voy. Cour eur. D.H., arrêt *Huvig*, précité, p. 41, § 8 et p. 52, § 25; pour les perquisitions, voy. Cour eur. D.H., arrêt *Niemietz* du 16 décembre 1992, série A, n° 251, p. 33, § 29; Cour eur. D.H., arrêt *Chappell* du 30 mars 1989, série A, n° 152-A, pp. 12-13, § 26). Par ailleurs, la proposition de directive RNIS va plus loin dans la mesure où elle tend à protéger les personnes morales non pas simplement en ce que le traitement de données y relatif conduirait à traiter des données personnelles, mais dans la mesure où les personnes morales elles-mêmes auraient un intérêt légitime à être protégées pour elles-mêmes (voy. proposition de directive du Parlement européenne et du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le secteur des télécommunications, en particulier des réseaux numériques à intégration de service (RNIS) et des réseaux mobiles numériques, précitée, art. 1, §2).

(31) La résolution du problème semble donc être laissée à la discrétion des États (voy. The Data Protection Registrar, *Questions to answers- Data protection and the EU Directive 95/46/EC*, Cheshire (U.K.), Office of the Data Protection Registrar, april 1996, p. 19). Concernant la Convention n° 108, le Comité consultatif a estimé d'une part que les parties étaient libres de l'appliquer aux personnes décédées (T-PD (94)7, p. 5), d'autre part que ce texte s'applique aux foetus (T-PD (95)3. p.5). À noter que l'article 4.5 de la recommandation R (97) 5 du Conseil de l'Europe relative à la protection des données médicales (précitée) étend la protection des données aux données de l'enfant à naître afin d'éviter, comme le précise le paragraphe 87 de l'annexe, que les données médicales d'un enfant ne soient publiques au moment de sa naissance.

(32) Le rapport explicatif de la Convention n° 108 précise qu'on parlera de données personnelles lorsqu'une personne est facilement identifiable. Cela ne couvre pas l'identification des personnes par des méthodes très complexes. Une telle définition n'est plus tenable, eu égard aux possibilité informatiques de déchiffrement des mesures de cryptage ou de brouillage complexes. Comme le souligne le paragraphe 27 de l'annexe du projet de recommandation statistique du Conseil de l'Europe (CJ PD (97) 20), des données individuelles apparemment anonymes peuvent s'avérer indirectement identifiables par la combinaison de données.

cluait les données rendues anonymes[33] par référence au critère des efforts excessifs nécessaires pour l'identification. Dans sa seconde version, le texte ne visait plus que les données agrégées sous forme statistique dès lors que les personnes concernées n'étaient plus raisonnablement identifiables[34]. Le texte actuel est dépourvu de toute précision. Le considérant 26 indique cependant que «pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne». Il ajoute en outre que la protection n'est pas accordée aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable. Il paraît permettre aux États membres de préciser plus avant l'exception en indiquant que les codes de conduite pourraient venir préciser les moyens à utiliser pour l'anonymisation.

13. – Une difficulté surgit lorsque des moyens matériels et techniques existent aux fins d'identifier les personnes concernées alors même qu'ils ne sont pas utilisés car l'identification n'est pas nécessaire à l'activité poursuivie. Deux interprétations peuvent s'opposer.

On peut considérer que les données sont identifiables et que la protection doit être respectée. On opte alors pour la protection la plus étendue en se justifiant en termes de risque: le risque d'identification justifie par lui seul une application de la réglementation. Ce faisant, on soumet les responsables à des obligations parfois très lourdes et on crée le risque de les amener à franchir l'étape d'identification.

On peut, à l'opposé, se placer *in concreto* dans le chef de l'utilisateur des données pour apprécier en fait sa situation. Le texte français de la directive[35] y invite dès lors qu'il semble introduire une présomption. Dès lors que, techniquement, *in abstracto*, un moyen existe de rendre les personnes concernées identifiables, elles sont *réputées* telles par la définition. Le caractère identifiable apparaît alors comme relatif eu égard aux possibilités d'identification du ou des responsables. Il revient, dans cette optique, à la personne qui traite les données et qui considère ne pas devoir respecter les principes protecteurs, de rapporter la preuve du caractère anonyme de celles-ci dans son chef, en présentant toute garantie utile quant à la conservation du caractère anonyme des données[36] et susceptible de rencontrer les critères retenus par la législation nationale pour conclure à la perte du caractère identifiable des données[37].

Cette dernière position paraît être la plus réaliste. Elle responsabilise l'utilisateur des données sur qui va reposer la charge de la preuve du caractère non identifiable des données. Elle présente toutefois des difficultés en pratique car l'utilisateur doit rapporter la preuve d'un fait négatif au moyen de critères par essence difficiles à rapporter.

B. – Le traitement de données à caractère personnel

14. – L'article 2, *b*, de la directive définit le traitement de données à caractère personnel comme suit: «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»[38].

Cette définition présente un champ d'application remarquablement large. On peut dire que toute ou ensemble d'opération(s), automatisée(s) ou non, portant sur des données à caractère personnel est visée de la collecte à l'effacement ou la destruction de celles-ci.

Elle n'implique pas d'elle-même une structuration particulière de l'information. Il en résulte que de l'information brute, présente par exemple dans un texte accessible sur un site Web, fait l'objet d'un traitement dès lors qu'elle fait l'objet d'une des opérations prévues (conservation, communication, etc.).

15. – La mise en œuvre d'une telle définition suppose toutefois qu'il soit possible d'identifier, en pratique, l'existence d'un traitement spécifique. Un effort de systématisation paraît dès lors nécessaire pour apprécier la portée de cette définition.

Un traitement, quel qu'il soit, vise toujours une finalité d'utilisation précise, distincte de l'ensemble des opérations techniques effectuées. Une collecte de données, par exemple via un formulaire papier ou l'enregistrement d'informations sur un site Web, sera effectuée en vue d'opérations de marketing ultérieures. La mise en place d'un call center permettra à une entreprise d'assurances de collecter les informations transmises par l'assuré suite à un sinistre afin de le gérer. La consultation d'un site Web, reprenant par exemple, les avocats établi dans un État, tendra à une collecte d'informations à insérer dans un fichier d'adresses de contacts. Le traitement est alors constitué de l'ensemble des opérations matérielles effectuées en vue de la réalisation de la finalité recherchée.

Cette constatation a permis à de nombreux États de considérer dans leur législation interne ou dans l'interprétation des définitions que le critère de distinction d'un traitement résidait dans la finalité poursuivie par le responsable du traitement. La directive ne remet pas en cause cette conception[39].

16. – Toute opération, même unique, suffit pour que l'on puisse distinguer un traitement. Ainsi, la consultation d'informations contenues dans une banque de données ou dans un texte accessible sur un site Web, sans enregistrement ultérieur, peut constituer un traitement[40].

Une telle conception, résultante d'un élargissement à outrance de la définition de traitement, aboutit à la mise en place d'une protection illusoire et affaiblit d'autant le système mis en place. En effet, elle conduit à imposer des obligations impossibles à respecter à défaut d'enregistrement et de conservation des données. Ainsi, comment la personne concernée pourrait-elle exercer ses droits d'accès et de rectification si les données ont été simplement consultées ou communiquées par un tiers sans que ce dernier ne les conserve? Quel serait l'objet d'un contrôle éventuel des autorités compétentes.

Exclure une opération unique comme la simple consultation ou la transmission[41] de don-

(33) Ce qui supposait «une modification des données à caractère personnel de sorte que les informations qui y sont contenues ne peuvent plus être associées à une personne physique déterminée ou déterminable, ou moyennant seulement un effort excessif en personnel, en frais et en temps».
(34) Pour visualiser le texte du projet initial au regard du second projet modifié, voy. la proposition modifiée de directive du Conseil 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, *J.O.C.E.*, n° C 311/30, du 27 novembre 1992.
(35) La version néerlandaise est conforme également à cette interprétation alors que la version anglaise paraît s'y opposer.
(36) En mettant par exemple en exergue la mise en place d'un système permanent de codage, cryptage ou brouillage excluant la possibilité pour l'entreprise d'identifier les personnes concernées, en s'engageant dans un code de conduite ou contractuellement lors de la collecte à conserver le caractère anonyme, etc.
(37) Les mêmes données pourraient être relatives à des personnes identifiables pour un responsable qui a les moyens nécessaires pour ce faire et rester anonymes pour d'autres, qui en sont dépourvus. Il paraît *a priori* raisonnable de dire que la réglementation ne s'applique qu'au premier et non aux seconds. Il convient en effet de ne pas confondre le problème de la définition des données à caractère personnel – données relative à une personne identifiée ou identifiable – et celui de la détermination du champ de la présomption introduite par la seconde partie de l'article 2.a. (sont réputées identifiables [...]) (*Contra* voy. P. De Hert, O. De Schutter, S. Gutwirth, «Pour une réglementation de la vidéosurveillance», *op. cit.*, p. 576, n° 25; S. Louveaux, «Article-by-article guide to Directive 95/46/C.E.», in: *The informed View, A business guide to changes in European data protection legislation*, novembre 1996, p. 3).
(38) L'article 2, *c*, de la Convention n° 108 définit le traitement automatisé «comme les opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés: enregistrement des données, application à des données d'opérations logiques et/ou arithmétiques, leur modification, leur effacement, extraction ou diffusion». Comme le précise le paragraphe 31 du Rapport explicatif, cette définition exclut la collecte, sauf si celle-ci est effectuée à des fins d'enregistrement.
(39) Le fait que dans certaines dispositions relatives au droit d'information et d'accès – art. 10, *b*, 11, *b*, 12, *a* – la directive parle des «finalités du traitement» est sans conséquence sur la détermination des traitements dès lors que les principes relatifs à la licéité et à la légitimité des traitements visent clairement chaque finalité distincte d'un traitement (cfr *infra*).
(40) Le paragraphe 31, alinéa 3, du Rapport explicatif de la Convention n° 108 inclut la consultation dans la notion de traitement, pour autant, selon l'interprétation dominante, que cette consultation s'accompagne d'un enregistrement des données.
(41) Article 1, § 3, de la loi belge: «tout ensemble

nées n'a pas comme conséquence de laisser la personne concernée par les données en dehors de toute protection efficace. Cette dernière peut non seulement se retourner contre le responsable du traitement qui met les données à la disposition d'autrui sur la base de la législation protectrice des données, mais également contre la personne qui utiliserait les données sans qu'un traitement n'apparaisse au sens de la réglementation et cela, en vertu des principes du droit commun (violation du droit au respect de la vie privée, du droit à l'image, du secret de la correspondance etc.). Si cette dernière introduit les informations dans un processus de traitement propre – par exemple en déchargeant tout ou partie des informations consultées dans ses propres banques de données –, la personne concernée retrouve l'intégralité de la protection accordée par la directive.

Il convient de remarquer que la première version du texte ne prévoyait pas que toute opération soit susceptible de constituer un traitement. Le texte actuel n'est apparu que dans la seconde version intégrant la collecte parmi les différentes opérations. On a voulu par là reconnaître à la personne concernée une protection complète dès la saisine des données par autrui même si leur traitement réel n'intervient que bien plus tard. Il a dès lors pu être jugé utile de préciser qu'une seule opération – sous-entendu la collecte – pouvait être considérée comme un traitement de manière anticipative. Ainsi, tout le processus de traitement est visé. On ne perçoit cependant pas de volonté des auteurs de la directive de retenir l'existence d'un traitement pour chaque opération unique.

C. – Fichiers de données à caractère personnel

17. – L'article 1, *c*, de la directive définit le fichier de données à caractère personnel comme étant «tout ensemble structuré de données à caractère personnel, accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique»[43].

Cette définition est prévue dans le seul but de préciser la portée ou l'exclusion de certaines obligations relatives aux traitements non automatisés[44]. En effet, ces derniers ne tombent sous le champ d'application de la directive que si les données sont «contenues ou appelées à figurer dans un fichier»[45]. On exclut ainsi, comme dans la plupart des législations nationales, les dossiers non structurés du champ d'application de la directive.

Le critère de distinction entre le dossier et le fichier est à trouver dans le degré d'accessibilité des données à caractère personnel. La structuration de l'information à prendre en compte est centrée sur l'existence de critères relatifs aux personnes concernées[46]. Ainsi, un dossier rangé selon un critère nominatif devrait être considéré comme un fichier. La directive ne précise cependant pas «les éléments d'un ensemble structuré de données à caractère personnel et les différents critères régissant l'accès à cet ensemble»[47]. Il revient donc à chaque État de les déterminer.

Le considérant 27 précise bien que «les dossiers ou ensemble de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application de la présente directive». On doute toutefois que ces «précisions» fassent taire toute controverse à ce propos. Le nœud du problème réside encore et toujours dans la nécessaire détermination de critères d'accessibilité applicables[48]. Aucune législation ne paraît avoir, à ce jour, offert de solution excluant toute discussion...

D. – Le responsable du traitement et le sous-traitant

18. – En vertu de l'article 2, *d*, de la directive, le responsable du traitement est «la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire»[49].

La définition reprise par la directive est classique et analogue à celle présente dans les législations nationales. Il s'agit de la personne responsable des choix qui président à la définition et à la mise en œuvre des traitements. Ces choix sont relatifs aux finalités et aux moyens utilisés. Si différentes personnes ou autorités déterminent conjointement ces éléments, elles seront chacune considérées comme responsables.

Le responsable du traitement doit cependant être distingué des personnes qui procèdent aux opérations de traitement en conformité à ses instructions. Celui-ci peut ainsi faire traiter les données par les membres de son personnel ou par un sous-traitant, personne juridiquement distincte mais agissant pour son compte[50]

Si une législation ou une réglementation nationale ou communautaire précise les critères précités, elle peut en outre déterminer des modalités particulières de désignation du responsable.

E. – Le tiers et le destinataire des données

19. – Le tiers est défini par l'article 2, *f*, de la directive comme toute personne autre que le responsable, le sous-traitant et les personnes placées sous leur autorité directe[51].

Il peut s'agir d'une personne physique ou morale, d'une autorité publique, d'un service ou de tout autre organisme. Dès lors que le responsable n'est pas la société elle-même ou le titulaire hiérarchique supérieur d'une entité étatique ou fédérée, un autre service ou organisme doit être considéré comme un tiers. Il en résulte par exemple que si le responsable d'un traitement est le chef du service personnel d'une société, les membres du service marketing sont considérés comme tiers.

Le tiers est parfois le destinataire des données mais pas nécessairement. Le destinataire vise toute personne qui reçoit communication des données qu'il soit ou non un tiers[54]. Les membres du personnel qui accèdent aux données dans le cadre de leur fonction sont donc des destinataires. Le texte de la directive prévoit cependant une exception en faveur des autorités «susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière». La notion de destinataire étant principalement utilisée pour déterminer le contenu des obligations d'information de la

d'opérations réalisées en tout ou partie à l'aide de procédés automatisés et relatif à l'enregistrement et la conservation de données à caractère personnel, ainsi qu'à la modification, l'effacement, la consultation ou la diffusion de ces données».

(42) Le considérant 47 de la directive estime, dans le même ordre d'idées, que celui qui transmet des messages contenant des données à caractère personnel – service de télécommunication ou de courrier électronique, dont le seul objet est de transmettre des messages de ce type n'est pas un responsable du traitement. Plus fondamentalement, ce n'est pas tellement sa qualité de responsable qui paraît pouvoir être déniée – il détermine sa finalité, le transport, et les moyens techniques pour ce faire – mais bien l'inexistence d'un traitement.

(43) L'article 2, *b*, de la Convention n° 108 définit le fichier automatisé comme «tout ensemble d'informations faisant l'objet d'un traitment automatisé». Le paragraphe 30 du Rapport explicatif précie que cette défintion «couvre non seulement des fichiers consistant en des ensembles compacts de données mais aussi des ensembles de données qui sont répartis géographiquement et réunis par l'intermédiaire d'un système automatisé à des fins de traitment». La seule différence introduite par la directive consiste à dire que l'ensemble d'informations doit être structuré.

(44) L'article 18, § 1, ne prévoit les modalités de notification à l'autorité de contrôle que pour les seuls traitements automatisés entièrement ou partiellement même si les traitements non automatisés peuvent être soumis à une telle obligation par les législations nationales; voy. également l'article 21 relatif à la publicité des traitements.

(45) Article 3, § 1, de la directive.

(46) Voy. le considérant 27 de la directive.

(47) *Idem.*

(48) Le problème se complique d'ailleurs si l'on se souvient qu'en pratique, fichiers manuels, dossiers et traitements automatisés sont étroitement liés entre eux. Ainsi, des dossiers sans véritable structure interne peuvent, via par exemple des numéros de classement et des noms, être reliés à des véritables traitements automatisés (par exemple les logiciels de gestion de la clientèle des avocats).

(49) L'article 2, *d*, de la convention n°108 définti le maître du fichier comme étant «la personne physique ou morale, l'autorité publique, le serivce ou tout autre organisme qui est compétent selon la loi nantionale pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractrèer personnel doivent être enregsitrées et quelles opérations leur seront appliquées».

(50) Article 2, *e*, de la directive: «La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement». À noter que l'article 2, *e*, parle de sous-traitement alors qu'il faut manifestement entendre sous-traitant. Cette notion est également une nouveauté par rapport à la Convention n° 108.

(51) La Convention n° 108 ne définit pas la notion de tiers.

(52) Article 2, *g*, de la directive.

personne concernée, il s'agit vraisemblablement d'éviter au responsable du traitement de devoir rappeler à la personne concernée que, par exemple, les agents du fisc, de la sécurité sociale, etc., spécialement habilités pour ce faire, sont susceptibles d'opérer des contrôles sur les informations traitées.

F. – Le consentement de la personne concernée

20. – On verra que le consentement de la personne concernée joue un rôle essentiel dans la protection mise en place. Il permet sous certaines conditions de légitimer un traitement ou de lever l'interdiction de traitement des données sensibles.

L'article 2, *h*, de la directive le définit comme «toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement»[53].

Toute manifestation de volonté peut constituer un consentement. Cela implique qu'il ne doit pas nécessairement être donné par écrit et qu'il peut être implicite, sauf exception prévue par la directive[54].

Le consentement doit être libre, c'est-à-dire être donné en dehors de toute pression. L'idée est de prévenir toute menace de discrimination suite au choix de la personne concernée. Cette condition, outre qu'elle peut difficilement être vérifiée, paraît bien illusoire en pratique. La pression économique consistant dans le risque de se voir refuser un produit ou un service considérés à tort ou à raison comme essentiels par la personne concernée l'amènera bien souvent à donner son consentement sans aucun esprit critique.

Le consentement doit également être spécifique. Il ne peut avoir un objet général, mais doit porter sur des traitements précisément définis notamment en leurs finalités, poursuivies par des responsables déterminés.

Le consentement doit enfin être informé. Le responsable du traitement doit donc transmettre à la personne concernée toute information nécessaire à l'analyse du risque particulier que représente le traitement envisagé pour ses droits et libertés. À cet égard, l'information reçue par la personne concernée au moment de la collecte semble constituer un minimum.

G. – Champ d'application matériel

21. – L'article 3 de la directive détermine son champ d'application matériel.

L'article 3, § 1, énonce que la protection vise tant les traitements de données à caractère personnel automatisés, en tout ou en partie, que les traitements non automatisés de données contenues ou appelées à figurer dans un fichier[55].

L'article 3, § 2, énumère les exceptions au champ d'application. Les traitements poursuivant des finalités purement personnelles ou domestiques ne sont pas visées. De manière générale, les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités relatives au droit pénal sont également exclus. Plus spécifiquement, les domaines qui relèvent des titres V (politique étrangère et la sécurité commune) et VI (coopération dans les domaines de la justice et des affaires intérieures, dit «troisième pilier») du traité sur l'Union européenne ne sont pas couverts. La protection des données est régie dans ces matières par des règles autonomes.

22. – Ainsi en ce qui concerne le troisième pilier, l'article K.2 du titre VI du traité de Maastricht dispose que la politique d'asile, la politique d'immigration, l'entrée des ressortissants des pays tiers, la lutte contre la toxicomanie, la coopération judiciaire en matière civile, en matière pénale, la coopération douanière et policière seront traitées par les États membres comme des questions d'intérêt commun et l'article K.3 ajoute que les États veilleront à coordonner leur action en arrêtant des positions communes, en adoptant des actions communes et en établissant des conventions[56].

III. – LIGNES DIRECTRICES DE LA PROTECTION

23. – L'article 6 de la directive, intitulé «Principes relatifs à la qualité des données»[57], permettra l'analyse des principes de base de la protection: loyauté (3.A), finalité (3.B), qualité des données (3.C)[58] et légitimation des traitements (3.D).

Les régimes spécifiques aux données dites «sensibles» et aux finalités fondées sur la liberté d'expression seront ensuite examinés (3.E).

A. – Le principe de loyauté

24. – L'article 6, *a*, dispose que les données doivent être traitées loyalement et licitement[59].

Pour être *licite*, un traitement de données doit respecter l'ensemble des prescrits légaux découlant de la directive. La *loyauté* du traitement évoque, quant à elle, la transparence des actions. Cette transparence doit être assurée dès la collecte, notamment par le biais de l'obligation d'informer la personne concernée. Ces dernières doivent savoir quel est le but d'utilisation des données, entre quelles mains elles se trouvent, à quelles fins elles sont communiquées. Lorsque des données sont destinées à être traitées hors du territoire communautaire, le traitement ne devrait être considéré comme loyal que si l'on informe les personnes concernées des destinataires ou des catégories de destinataires des données[60].

B. – Le principe de finalité

25. – La doctrine a souligné l'importance du principe de finalité du traitement pour la protection de la vie privée. Ce principe repose sur le postulat que la menace pour la vie privée que constituent les traitements de données à caractère personnel réside davantage dans la finalité qu'ils poursuivent que dans la nature des données traitées[61]. C'est en outre «à partir de la finalité d'un traitement que tout un faisceau d'exigences est formulé quant à la nature des données enregistrées, à leur durée de conservation et à la qualité de leur destinataire»[62].

a. – La finalité doit être déterminée et explicite

26. – L'article 6, *b*, précise que les données doivent être collectées pour des finalités déterminées et explicites. *A contrario*, un traitement mis en œuvre «à toutes fins utiles» ou sans but précis n'est pas autorisé. Une finalité implicite doit également être exclue. Cette obligation de déterminer la finalité poursuit trois objectifs: délimiter l'atteinte aux droits et libertés individuelles, assurer la transparence du traitement et en permettre le contrôle. Diverses obligations particulières viendront concrétiser cette obligation (cfr *infra*, en particulier les obligations d'information des personnes concernées et de notification).

(La deuxième partie paraîtra dans le *J.T.D.E.* de septembre 1997)

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

(53) La Convention n° 108 ne recourt pas à la notion de consentement, mais différentes recommandations l'utilisent, telle par exemple la recommandation R (97) 5 sur la protection des données médicales.
(54) Par exemple en matière de données dites sensibles (cfr *infra*).
(55) L'article 3, § 1, de la Convention n° 108 limite l'application de ce texte «aux fichiers et aux traitments automatisés de données à caractèer personnel dans les secteurs publics et privés».
(56) L'article 14 de la Convention Europol précitée, de même que le dernier considérant du projet de Convention Eurodac, se réfèrent à la Convention n° 108. L'article 126 de la Convention d'Application de Schengen y renvoie aussi. La Convention n° 108 apparaît dès lors comme le socle commun des textes européens relatifs à la protection des données.
(57) Ce titre est la transcription littérale de celui de l'article 5 de la Convention n° 108.
(58) Notons dès à présent que l'article 13 permet aux États membres de prendre des mesures visant à limiter la portée de ces trois premiers principes. Ces limitations n'étant pas propres à ceux-ci, elles seront examinées gobalement *infra*.
(59) L'article 5, *a*, de Convention n° 108 prévoit, quant à lui, que les données doivent être «obtenues et traitées loyalement et licitement». Cependant, dans la mesure où l'article 2 de la directive englobe la collecte dans la notion de traitement, on peut considérer que l'article 6, *a*, de la directive et l'article 5, *a*, de la Convention n° 108 ont une portée identique.
(60) L'article 10 de la directive, qui règle le droit d'information de la personne concernée, dispose à cet égard que «compte tenu des circonstance , des informations supplémentaires devront être fournies pour assurer à l'égard de la personne concernée un traitement loyal des données».
(61) Voy. M.-H. BOULANGER, C. DE TERWANGNE et Th. LÉONARD, «La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel», *J. T.*, 1993, p. 377.
(62) Voy. CNIL, *Dix ans d'informatique et libertés*, Economica, Paris, 1988, pp. 81 et s.; voy. aussi S. GUTWIRTH, «De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992», *T.P.R.*, 1993, p. 1439.