

Libre circulation des données et protection de la vie privée dans l'espace européen

François RIGAUX

Introduction (*)

Le droit, comme l'informatique, se construit selon un rythme binaire. Entre deux réponses à une question, l'une évince l'autre selon la logique du tiers exclu: l'accusé est coupable ou innocent, un être humain est un homme ou une femme, il est marié ou célibataire, un contrat est valable ou nul. Certaines réalités humaines résistent aux procédés de taxinomie binaire: il y a du féminin en tout homme et du masculin en toute femme. L'orientation sexuelle n'est pas non plus aussi tranchée qu'il pourrait paraître selon la division en hétérosexuels et homosexuels. On pourrait multiplier les exemples.

La nécessité de tenir en équilibre deux intérêts divergents, sans qu'aucun ne puisse, en principe, être sacrifié à l'autre, apparaît dans l'intitulé de la directive 95/46/CE du Parlement et Conseil des Communautés européennes 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 données¹. La même paire apparaît dans l'intitulé de la présente contribution aux *Mélanges en l'honneur d'Ulrich Drobnig*. Ce n'est pas une division binaire qui les oppose. Il s'agit d'intérêts divergents sans doute mais que les auteurs de la norme prétendent concilier. L'un des objets de la présente étude sera de vérifier les limites d'un tel accommodement. L'« espace européen » auquel il est fait référence dans le même intitulé vise les deux principaux domaines scientifiques dans lesquels le Pr Drobnig s'est distingué : le droit international privé et la méthode comparative. Celle-ci a, en effet, été mise en œuvre pour l'harmonisation du droit à l'intérieur de la Communauté européenne, mais l'unification du droit n'a pas été à ce point complète qu'elle ait éliminé tout problème de conflit de lois.

À l'instar des instruments internationaux et des lois nationales qui l'ont précédée, la directive européenne prévoit l'institution d'autorités administratives indépendantes auxquelles le législateur étatique est invité à confier une mission de contrôle sur les banques de données à caractère personnel. Ainsi, la protection de droits individuels qui relèvent au premier chef de la sphère privée est assurée par des mécanismes de droit public, jetant, une fois de plus, le discrédit sur la division dogmatique entre le droit privé et le droit public.

La suite de cette étude aura pour objet les problèmes suivants:

- I/ Les divergences terminologiques
- II/ La discordance d'objectifs fondamentaux

* Ce texte ne donne pas toutes les notes de référence. Se reporter à l'article initialement publié dans *Festschrift für Ulrich Drobnig, zum siebzigsten Geburtstag*, publié ici avec l'autorisation de l'auteur et du Max Plank Institut für ausländisches und IPR, Hambourg. Le secrétariat du groupe « Société d'information et vie privée », à l'Académie, tient le texte intégral à la disposition des lecteurs

¹ JOCE, n° L. 281/31 du 23 novembre 1995.

- III/ Le recours a des concepts indéterminés et le renvoi à la pondération d'intérêts concurrents;
- IV/ L'immersion d'une nouvelle technologie dans des systèmes conceptuels préexistants;
- V/ Les conflits de normes et leur pacification;
- VI/ La détermination du domaine spatial du nouveau droit de l'informatique.

I/ LES INSTITUTIONS ET LES MOTS POUR LE DIRE

Un premier paradoxe est que les autorités de contrôle déjà existantes dans la plupart des pays européens exercent une activité qui est à peu près la même partout et a des visées identiques, alors que leurs fonctions ne sont pas désignées par les mêmes mots. Pareille divergence terminologique n'est sans doute pas sans portée. On peut y distinguer au moins trois orientations.

Ou bien le nom de l'autorité de contrôle désigne clairement l'objet et l'étendue de ses compétences : la protection de la personne à l'égard du traitement de données à caractère personnel. L'article 30 de la loi italienne n° 675 du 31 décembre 1996, l'une des plus récentes en la matière, est un exemple de cette première famille de dénomination : *Garante per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*².

L'article 6 de la loi française du 6 janvier 1978 fait aussi, mais moins clairement sans doute, apparaître que le législateur a institué un organe nouveau chargé de la protection des libertés individuelles dans le domaine de l'informatique : *Commission nationale de l'informatique et des libertés*³.

Ou bien la fonction est énoncée en termes plus généraux que ne l'implique la législation qui l'a instituée. Tel est le cas, notamment, pour l'article 22 de la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, qui institue une « Commission de la protection de la vie privée » dont les compétences sont déterminées par les articles 29 à 31 de la loi sans qu'elles excèdent le secteur de cette protection, délimité en conformité avec l'intitulé de la loi⁴. Toutefois, le législateur a ultérieurement confié à la commission une compétence consultative en d'autres domaines de la vie privée⁵

Une troisième famille d'instruments législatifs désigne l'organe de contrôle par l'objet matériel de ses compétences, sans référence expresse à la volonté de protection des personnes. Le modèle en est procuré par les commissions de protection des données (*Datenschutzkommission*) des lois allemandes⁶ ou par la *Registratiekamer* qu'a instituée l'article 37 de la loi néerlandaise du 28 décembre

² Pareille désignation du « garant » reprend l'intitulé de la loi *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, *Gazzetta Ufficiale*, I, n. 3, 8 janvier 1997.

³ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique et aux libertés, *Journal officiel de la République française*, 7 janvier 1978, p. 227.

⁴ *Le Moniteur belge*, 18 mars 1993. En outre, avant le 8 décembre 1992, divers instruments de nature législative avaient déjà réglé la matière dans des secteurs particuliers. Voir, sur ce point : F. Rigaux, « La protection des banques de données et le respect de la vie privée », *Revue de droit de l'ULB*, 1994, n° 3, 51-71.

⁵ Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées (*Le Moniteur belge*, 24 janvier 1995), art. 14.

⁶ Selon le § 17 de la *Bundesdatenschutzgesetz* du 27 janvier 1977, *BGBI I*, S. 201 : « Es ist ein Bundesbeauftragter für den Datenschutz zu bestellen. » La loi de 1977 a été modifiée par la *Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes* du 20 décembre 1990 (*BGBII*, 2954), entrée en vigueur le 1^{er} Juin 1991.

1988⁷. Non moins que les précédentes, ces lois visent à la protection des personnes dont les données sont traitées par un procédé informatique, mais il reste que l'expression *Datenschutz* n'est pas dépourvue d'équivoque, Les données sont une marchandise dont la protection ne rejoint pas nécessairement la protection des personnes qui devraient en principe maîtriser elles-mêmes leurs propres données⁸. En outre, alors qu'à l'origine seuls les traitements automatisés étaient soumis à des règles spécifiques⁹, le besoin est ensuite apparu d'étendre la protection aux fichiers manuels et aux « dossiers structurés »¹⁰.

II/ PROTECTION DES INDIVIDUS ET LIBRE CIRCULATION DES DONNÉES

Les politiques législatives nationales tendent à la protection de la population de l'État à l'égard des traitements (automatisés ou non) de données à caractère personnel¹¹. La transnationalisation et la délocalisation de l'outil informatique, la facilité avec laquelle les données passent les frontières ont très tôt fait apparaître la nécessité de soumettre les États à des normes communes. Deux organisations internationales, l'OCDE et le Conseil de l'Europe, ont, il y a quelque vingt ans, élaboré des textes qui convergent pour l'essentiel¹², en dépit des approches différentes qui y furent respectivement suivies.

Le Conseil de l'OCDE a adopté le 23 septembre 1980 une Recommandation concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. Cette recommandation a été publiée le 1^{er} octobre 1980, précédée d'une préface et suivie d'un exposé des motifs qui en éclaire la portée¹³. Les lignes directrices (*guidelines*) sont annexées à la Recommandation.

⁷ « Wet van 28 december 1988, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met persoonsregistratie (Wet persoonsregistratie) », *Staatsblad van het Koninkrijk der Nederlanden*, 1988, rit. 665. L'article 37, alinéa 2 de la loi définit les compétences de la « chambre d'enregistrement » : « De Kamer ziet toe op de werking van persoonsregistraties overeenkomstig het bij en krachtens deze wet bepaalde en in het belang van de bescherming van de persoonlijke levenssfeer in het algemeen. »

⁸ Le « droit à la maîtrise des données personnelles » (*Recht auf « informationelle Selbstbestimmung »*) a été tenu pour un droit constitutionnellement garanti (BVerfG, 15 décembre 1983, *BVerfGE*, 65, 1, 43).

⁹ Tel était, par exemple, l'objet limité de la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Mais l'article 3, 3, c de la Convention permettait aux États d'en étendre l'application aux traitements non automatisés. Plusieurs dispositions de la loi belge du 8 décembre 1992 s'appliquent aux fichiers manuels.

¹⁰ Voir en ce sens le considérant (27) de la directive 95/46/CE du Parlement 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*, n°, L. 281/31 du 23 novembre 1995). L'article 3, 1 de la directive en étend l'application au « traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ». À la lumière du considérant précité, il faut inclure les dossiers structurés parmi les fichiers. La distinction évasive entre un dossier ou un ensemble de dossiers et un fichier a fait l'objet d'observations du Conseil d'État et de la Commission de la vie privée au cours des travaux préparatoires de la loi du 8 décembre 1992 (voir F. Rigaux, *op. cit.*, n. 4, n° 8).

¹¹ Tant dans le texte de la Convention du 28 janvier 1981 (note 9) que dans celui de la directive du 24 octobre 1995 (note 10), l'expression « données à caractère personnel » désigne « toute information concernant une personne physique identifiée ou identifiable ». La même notion est exprimée dans le texte anglais par « *personal data* », qui ne peut dès lors être traduit par « données personnelles ». La terminologie italienne est, sur ce point, plus proche de l'anglaise que de la française.

¹² La convergence n'est pas fortuite. A l'exception de Chypre et de Malte, tous les États membres du Conseil de l'Europe (en 1980) étaient aussi membres de l'Organisation de coopération et de développement économique (OCDE), qui inclut en outre cinq États non européens, l'Australie, le Canada, les États-Unis, le Japon et la Nouvelle-Zélande.

¹³ *Publication de l'OCDE*, Paris, 1980, 42 p.

Datant du 28 janvier 1981, la Convention du Conseil de l'Europe (*supra*, n. 5, p. 27) est de nature plus contraignante, bien que les dispositions qu'elle contient ne soient pas directement applicables (art. 4, 1). Sur ce point, elle n'est pas sans analogie avec la directive communautaire déjà citée (*supra*, n. 6, p. 27).

Ce qui distingue le plus la Recommandation de l'OCDE de la Convention du Conseil de l'Europe est une question d'accent. Sans doute l'une comme l'autre s'efforcent-elles de « concilier des valeurs à la fois fondamentales et antagonistes, telles que le respect de la vie privée et la libre circulation de l'information », ainsi qu'il est écrit au début du préambule de la Recommandation et dans le dernier considérant de la Convention. En revanche, les autres motifs de chacun des deux préambules insistent sur une seule des deux « valeurs » jugées antagonistes : les deux premiers considérants du préambule de la Convention réaffirment la prééminence du respect des droits de l'homme et des libertés fondamentales, tandis que les trois derniers alinéas du préambule de la Recommandation insistent sur la contribution des flux transfrontières au développement économique et social¹⁴.

Bien que la Communauté européenne soit au premier chef une organisation économique, la directive du 24 octobre 1995 s'efforce à une présentation plus équilibrée des deux objectifs qu'elle vise : « Respecter les libertés et droits fondamentaux [des] personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus. »¹⁵

Alors que l'hypothèse même d'une circulation transfrontières des données était plutôt perçue avec inquiétude par les premières lois nationales de régulation, elle forme la substance même des instruments internationaux ou communautaires, l'harmonisation des normes protectrices sous la garantie du respect de certains principes fondamentaux étant la condition nécessaire, mais jugée suffisante, de la libre circulation des données. Le considérant (11) de la directive rappelle encore que ces principes se laissent déjà déduire de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950. Cela signifie que la victime individuelle d'une violation du droit au respect de la vie privée peut adresser à la Commission européenne des droits de l'homme une requête dirigée contre l'État qui pourrait en être tenu responsable¹⁶.

En dépit des formulations balancées s'efforçant de concilier des objectifs antagonistes, force est de constater que tous les instruments actuellement en vigueur, qu'ils soient nationaux, internationaux ou communautaires, sont traversés par le conflit de plusieurs libertés, la liberté de l'information, la liberté du commerce et des échanges, la liberté de la vie privée sous la forme spécifique de la maîtrise par chaque sujet des données relatives à sa personne, à son histoire, ses activités, ses

¹⁴ Pour une comparaison plus détaillée des deux instruments, voir, notamment: F. Rigaux, « La loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractère personnel », *Rev. crit. dip.*, 1980, 443-478, nos 13-17.

¹⁵ Préambule, considérant (2). Les considérants (3) à (11) maintiennent cette rédaction balancée avec, toutefois, une insistance répétée sur les exigences du « marché intérieur », lequel implique la libre circulation des données, selon le considérant (3).

¹⁶ Parmi les instruments internationaux, on signalera encore la Convention d'application de l'accord de Schengen du 14 juin 1986 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la France, relatif à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990. La Convention d'application est actuellement en vigueur entre les États qui l'ont conclue, auxquels se sont joints l'Autriche, l'Espagne, la Grèce, l'Italie et le Portugal. Le chapitre II (art. 93 à 101) a pour objet l'exploitation et l'utilisation du Système d'information Schengen, tandis que le chapitre III veille à la protection des données à caractère personnel (art. 102 à 118). La fiabilité et la sécurité des données priment le droit au respect de la vie privée sans totalement l'évincer. Voir, notamment : Lucia Serena Rossi, « La protezione dei dati personali negli accordi di Schengen alla luce degli standard fissati dal Consiglio d'Europa », in *Da Schengen a Maastricht*, ed. Bruno Nascimbene, Milano, Giuffrè, 1995, p. 173-201.

opinions, sa religion, sa vie familiale, ses maladies, les infractions dont il a été accusé ou convaincu. De nombreux articles de la directive communautaire portent la trace de l'indécision du législateur et révèlent l'impossibilité de régler la matière par des normes préétablies, sûres et contraignantes.

III/ LES CONCEPTS INDÉTERMINÉS ET LES RÈGLES CONDITIONNELLES

L'ambivalence d'objectifs plus contradictoires que complémentaires entraîne des hésitations dans la rédaction des textes et l'accumulation d'incertitudes qui vont bien au-delà du recours occasionnel à des concepts indéterminés (*unbestimmte Begriffe*). Plusieurs articles de la directive communautaire et davantage encore le préambule illustrent ces observations.

En dépit du projet ambitieux annoncé dans le considérant (11) de la directive, aux termes duquel « les principes [...] contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la Convention, du 28 janvier 1981, du Conseil de l'Europe... », la directive abonde en normes conditionnelles. Citons quelques exemples.

Contenant plusieurs « principes relatifs à la légitimation des traitements de données », l'article 7 prévoit une série de légitimations alternatives dont la dernière pourrait supplanter toutes les autres. En effet, à la lettre *f*) il est écrit que le traitement de données à caractère personnel peut être effectué si :

il 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, qui appellent une protection au titre de l'article 1^{er}, § 1.

Le considérant (30) contient quelques indications sur la nature des activités qui pourraient justifier l'intérêt légitime requis, mais il reste incertain si le législateur étatique peut se borner à introduire dans son ordre interne une norme reproduisant la double indétermination contenue dans le texte communautaire reproduit ci-dessus : quelle est l'étendue des intérêts « légitimes » ainsi ajoutés aux justifications plus précises des lettres a à e du même article, et, surtout, en quoi la référence aux termes très généraux de la garantie procurée par l'article 1^{er}, alinéa 1^{er}, va-t-elle circonscrire l'équilibre à maintenir avec un intérêt tenu pour légitime. Il est douteux qu'aucun législateur soit en mesure de préciser la portée d'un texte aussi vague, qui se borne à poser un problème sans y apporter de solution. Il appartiendra sans doute aux autorités de contrôle, nationales et communautaire, le cas échéant aux cours et tribunaux et, en dernière analyse, à la Cour de justice, de se prononcer sur l'interprétation du texte à la lumière des litiges particuliers qui leur seront soumis¹⁷.

L'article 7 *f*) est particulièrement significatif parce qu'il met en balance deux notions indéterminées: un intérêt qualifié de légitime (alors qu'on attendrait plutôt du législateur qu'il distinguât ce qui est légitime de ce qui ne l'est pas) et le seul principe du droit au respect de la vie privée. Mais d'autres articles de la directive recourent aussi à des concepts peu ou non déterminés, tels l'article 11, alinéa 2 (« l'information de la personne concernée se révèle impossible ou implique des

¹⁷ Bien que la Cour, saisie d'une question préjudicielle d'interprétation du droit communautaire, soit sans compétence pour se prononcer sur l'application du texte à un litige particulier, elle ne laisse pas de prendre en considération les particularités du cas litigieux pour formuler sa propre interprétation. Comp. Ulrich Damman et Spiros Simitis, *EG-Datenschutzrichtlinie* (Baden-Baden, Nomos Verlagsgesellschaft, 1997), p. 152-153, avec une note de scepticisme quant à la possibilité d'atteindre à l'harmonie par cette méthode.

efforts disproportionnés ») ou l'article 13, alinéa 2 (« dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée »).

IV/ L'INSERTION DES PRINCIPES DE DROIT COMMUNAUTAIRE DANS LES SYSTÈMES CONCEPTUELS DE DROIT INTERNE

À l'instar des instruments internationaux d'harmonisation du droit interne, la directive utilise des concepts dont la résonance en chacun des ordres étatiques où ils seront mis en œuvre dépendra du sens qu'ils sont aptes à y recevoir. Le noyau de la plupart de ces concepts est certes commun à tous les États destinataires de la directive sans que les contenus en soient pour autant identiques. Les concepts de consentement et de responsabilité sont particulièrement significatifs à cet égard.

Modalités diverses du consentement

Affirmé par le Tribunal constitutionnel fédéral allemand (supra, n. 4, p. 27), le principe du « droit à l'autodétermination informationnelle » devrait entraîner que tout enregistrement de données fût subordonné au consentement de la personne identifiée ou identifiable à laquelle se réfèrent les informations recueillies. L'importance de la question est telle que l'article 2 h) de la directive contient une définition du consentement à laquelle on ne trouve guère de parallèle dans les Codes civils usuels :

Aux fins de la présente directive, on entend par:

h) « consentement de la personne concernée » : 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 traitement¹⁸.

Non seulement chacune des trois épithètes qui qualifient la manifestation de volonté — et le mot « volonté » lui-même — nécessiterait une définition, mais quelque circonstanciée qu'elle fût, la définition initiale n'a pas paru suffisante, et la lettre a) de l'article 7 y ajoute une quatrième épithète, également peu habituelle en droit civil: que « la personne concernée a indubitablement donné son consentement ». L'adverbe signifie sans doute que le consentement doit obéir à une preuve particulièrement exigeante, mais on conçoit difficilement que la forme en laquelle l'exigence est formulée par la directive soit reproduite dans les mêmes termes dans la législation nationale : Qu'est-ce qu'un consentement dont il serait permis de douter ?

À l'article 8, qui a pour objet le traitement des « données sensibles »¹⁹, la notion de consentement apparaît accompagnée d'un autre qualificatif. La prohibition du

¹⁸ Dans leur commentaire de l'article 2b), Damman et Simitis insistent à plusieurs reprises sur un passage du texte allemand de cette disposition qui n'a pas d'équivalent exact dans les textes français et anglais : « Einwilligung der Betroffenen » est définie : « Jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt... » Dans les textes anglais et français, les mots

« für den konkreten Fall » ont été traduits par « spécifiques », *specific*, qui sont loin d'avoir la même portée. Comme la directive a été élaborée à l'époque de la présidence allemande de la Communauté, l'influence des juristes allemands sur sa rédaction a été, à tort ou à raison, avancée.

¹⁹ Pour une analyse critique de cette notion, voir notamment Spiros Simitis, « "Sensitive Daten" — Zur Geschichte und Wirkung einer Fiktion », *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini* (Verlag Stampfli und Cie AG, Berri, 1990), p. 469-493. Dans le commentaire récent de la directive cité à la note 1, p. 31, les auteurs critiquent assez sévèrement l'ensemble de l'article 8, « l'un des éléments les plus problématiques de la directive » (Damman/Simitis, p. 159). La notion de « données sensibles » est tenue pour « unidimensionnelle » et apparaît en conséquence comme trop englobante par certains aspects, insuffisante par d'autres (p. 160).

traitement des catégories de données énumérées à l'alinéa 1^{er} est levée lorsque « la personne concernée a donné son consentement explicite à un tel traitement... »²⁰. Le sens de l'épithète paraît ici assez clair : il faut que le consentement ait eu pour objet explicite le traitement de l'une des données énumérées à l'alinéa 111. Mais l'emploi de ce terme invite à poursuivre la réflexion sur le sens du caractère indubitable du consentement dans l'article 7, a) : un consentement peut-il recevoir cette qualification tout en étant implicite ? La réponse affirmative paraît la plus vraisemblable, surtout si l'on compare ces deux textes à une autre disposition, elle aussi d'origine communautaire, l'article 3, alinéa 1^{er}, de la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles²¹. Selon la deuxième phrase de cet alinéa, le choix par les parties de la loi applicable au contrat « doit être exprès ou résulter de façon certaine des dispositions du contrat ou des circonstances de la cause »²². Ainsi, un choix (ou un consentement) peut être implicite et certain, mais est-il, dans le même cas, indubitable ?

Aussi bien l'article 8, alinéa 2, que l'article 7 de la directive passent outre à l'absence de consentement exprimé selon les exigences respectives de la lettre a) de chacune de ces dispositions. Suit, en effet, une série d'hypothèses dans lesquelles le traitement « est nécessaire » à l'un ou l'autre des objectifs énumérés. Sans revenir sur l'article 7, f), qui énonce cette nécessité en des termes vagues au point d'être indistincts, on se bornera aux hypothèses où il est permis de présumer un consentement implicite. C'est le cas de l'article 7, b) et de l'article 8, alinéa 2, b). Selon le premier de ces textes, il est dérogé à l'exigence d'un consentement si 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.

Outre le contrat de travail, toute une gamme d'obligations contractuelles peut être envisagée : banque, assurance, transports, achat à crédit, emprunt, etc. Le concept de « nécessité » est, dans ce contexte, ambigu, car de tels contrats se sont, jusqu'à une époque récente, conclus et exécutés sans recours à un traitement informatisé, mais celui-ci est dorénavant requis par les techniques contemporaines de gestion des contrats. On conçoit malaisément que le client d'une banque ou d'une compagnie d'assurance, que le voyageur acquérant un billet d'avion exigent de leur cocontractant que toutes les informations relatives à ces opérations soient soustraites à un procédé d'enregistrement informatique. C'est en ce sens que le traitement de données à caractère personnel n'est pas seulement nécessaire, il est inéluctable, car celui qui prétendrait s'y soustraire se placerait en dehors de la vie sociale telle qu'elle est aujourd'hui organisée. Le degré et l'étendue de pareille nécessité ne sauraient être mesurés ni par un organe de contrôle ni par une juridiction, ils suivent inexorablement l'avancée des techniques et des pratiques informatiques.

L'article 8, alinéa 2 énumère cinq exceptions à la prohibition de traiter les données énumérées à l'alinéa 1^{er}. La lettre b) est rédigée dans les termes suivants :

b) le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la

²⁰ Mais le texte poursuit en ces termes : « Sauf dans les cas où la législation de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut être levée par le consentement de la personne concernée. »

²¹ JOCE, NrL 266/1 du 9 octobre 1980. Le texte a été publié en six langues (allemand, anglais, français, italien, néerlandais et danois) dans : *BGBl*, 1986, II, S. 810.

²² « The choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case. » On peut hésiter sur le point de savoir si « reasonable certainty » est l'équivalent exact de : « de façon certaine ». Le texte allemand porte : « mit hinreichender Sicherheit ».

mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates.

C'est donc ici un seul type de contrat qui est visé, le contrat de travail, et les précautions qui sont prises sont d'autant plus justifiées que la maîtrise de l'outil informatique vient renforcer le pouvoir traditionnellement exercé par le chef d'entreprise sur les travailleurs²³. L'état de dépendance où se trouvent ceux-ci, état qui ne peut que s'aggraver à une époque où le travail devient de plus en plus rare, est considérablement accru par la masse d'informations aisément accessibles dont disposent aujourd'hui les entreprises informatisées. Toutefois les précautions ne concernent que le traitement des données sensibles. Pour les autres données, il suffit, aux termes de l'article 7, b), que le traitement soit nécessaire. Mais on ne saurait, à cet égard, parler de révolution informatique, les instruments nouveaux se bornant à renforcer ou à rendre plus contraignant le lien de subordination qui demeure l'élément le plus caractéristique du contrat de travail. C'est donc aux lois organisant les relations de travail qu'il appartient d'établir les contrepoids rendus nécessaires par le surcroît d'efficacité conféré aux chefs d'entreprise.

Les règles de responsabilité

Les obligations mises à charge des responsables de traitements informatisés seraient de peu de poids si leur transgression ne devait entraîner des conséquences pour le contrevenant. Aux mesures administratives pouvant être arrêtées par l'autorité de contrôle et aux sanctions pénales que les États destinataires de la directive ont le devoir d'introduire dans leur ordre interne (art. 24) s'ajoute l'obligation de réparer le préjudice subi « du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive » (art. 23, al. 1^{er}). Le régime de responsabilité ainsi institué est assez complexe et suscite une série de questions qui ne pourront qu'être succinctement évoquées.

Une première série de problèmes concerne la source du droit de la responsabilité. La directive se borne à énoncer un principe assorti d'une exception inscrite dans l'alinéa 2:

Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

On pourra se demander si la non-imputabilité est la seule cause d'exemption ou si d'autres exonérations de responsabilité peuvent être puisées dans le droit interne²⁴.

Pour le surplus, les conditions de la responsabilité doivent être déterminées selon le droit interne de chaque État, ce qui fait apparaître deux questions, la première étant relative au choix de la loi applicable (on y reviendra plus loin), la seconde au contrôle exercé par la Cour de justice des Communautés européennes sur le niveau minimum de responsabilité que les États doivent garantir. Or, comme le révèle la jurisprudence de la Cour, d'abord sur la responsabilité de la Communauté et ensuite sur celle des États, certaines notions fondamentales du

²³ Damman et Simitis (note 17) donnent deux exemples d'hypothèses où l'enregistrement de données sensibles par l'employeur est licite : dans les entreprises de tendance et pour l'exécution de programmes visant à l'intégration des minorités (p. 164).

²⁴ Selon Damman et Simitis (note 17), les États pourront soit régler la question dans l'instrument législatif donnant exécution à la directive, soit modaliser le droit commun de la responsabilité (p. 262). Après avoir affirmé que le régime de la directive se situe à mi-chemin entre la responsabilité pour faute et le système du risque (p. 262), ils énoncent ensuite plus précisément qu'il s'agit d'une responsabilité objective tempérée par la preuve de l'absence de faute (p. 263).

droit de la responsabilité varient selon les États, et il n'est pas certain que la Cour elle-même manie les concepts avec la rigueur souhaitable. Parmi les problèmes on citera la réparation d'un dommage indirect et celle du manque à gagner (*lucrum cessans*). En ce qui concerne le premier point, l'arrêt du 5 mars 1996 (*Brasserie du pêcheur / Factortame*) exige un lien de causalité direct entre la faute et le dommage, tandis que d'autres arrêts prononcés à la même époque et également relatifs à la responsabilité de l'État requièrent un lien de causalité sans plus, ce qui paraît inclure la causalité indirecte²⁵. La mise en œuvre de l'article 23 de la directive suscitera un problème analogue.

Une dernière série de problèmes concerne la désignation du destinataire de l'obligation de réparer le préjudice. Selon les termes de la directive, c'est le « responsable du traitement », tel qu'il est défini par l'article 2, d) du même instrument. Mais il ne faudrait pas exclure les fautes personnelles d'individus ayant participé à la gestion du traitement ni celle de l'État s'il a été en défaut d'exécuter la directive ou en a fait une mise en œuvre incomplète ou incorrecte. Pareille responsabilité est entrée dans le droit communautaire depuis l'arrêt *Francovich* du 19 novembre 1991 (cité à la note 1. ci-dessous).

LES CONFLITS DE NORME ET LEUR PACIFICATION

Vie privée et liberté d'expression

Parmi les dispositions de la directive qui, de manière explicite, posent les termes d'un conflit d'intérêts ou de valeurs que le législateur étatique — et, plus vraisemblablement, le juge — auront à tâche de surmonter, l'article 9 occupe une place de choix. Les « exceptions et dérogations » au chapitre II de la directive que les Etats membres peuvent prévoir « pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique et littéraire » ne sont licites que « dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ». Sous sa forme classique, le conflit entre ce droit et cette liberté surgit quand un organe des médias a divulgué de manière illicite un fait relatif à la vie privée d'une personne. Dans l'article 9 de la directive, c'est d'un conflit au, second degré qu'il s'agit. Alors que l'élément de publicité est inhérent à l'atteinte à la vie privée et que de ce point de vue la récolte et le stockage d'informations dont la divulgation serait illicite ne sont pas par eux-mêmes illicites, c'est le traitement de telles données qui est visé par l'article 9. Sous couleur de faire une juste place à la garantie de la liberté d'expression, cette disposition pourrait y apporter une restriction nouvelle à travers le contrôle des sources des organes des médias. La différence est particulièrement notable en ce qui concerne les fichiers manuels qui entrent dans le champ d'application de la directive en vertu de l'article 3, alinéa 1^{er}. Afin de pouvoir satisfaire à bref délai aux nécessités de l'information, les organes des médias et les agences de presse emmagasinent un grand nombre d'informations qui ont en partie pour objet la vie privée des personnes. Or, jusqu'à présent, il n'était pas illicite de recueillir et de stocker ces informations, la prudence des organes des médias ne devant s'exercer qu'à l'occasion de leur dissémination. Le lecteur des notices nécrologiques publiées par les grands journaux anglais à l'occasion du décès d'un personnage public (*public figure*) y trouvent des informations souvent circonstanciées relatives à la vie familiale et aux incartades

²⁵ CJCE 5 mars 1996, aff. jointes C-46/93 et C-48/93, *Brasserie du pêcheur SA et République fédérale d'Allemagne, The Queen and Secretary of State for Transport ex parte Factortame Ltd*, Recueil I-1131, § 65, p. 1152. Comp. CJCE, 19 novembre 1991, aff. jointes C-6/90 et C-9/90, *Francovich et Bonifaci*, Recueil 1991, p. 5415, § 40 ; 14 juillet 1994, aff. C-91/92, *Faccini Dori*, Recueil I-3325, p. 3357, § 27 ; 8 octobre 1996, aff. jointes C-178/94, C-179/94 et C-190/94, *Dillenkofer*, § 27, § 29. Pour plus de développements, voir F. Rigaux, « La responsabilité de l'État selon le droit des Communautés européennes », note sous l'arrêt du 5 mars 1996, *Rev. crit. jur. belge*, 1997, 283-298.

sexuelles du défunt²⁶. Il est vraisemblable que les règles sur ce point varient d'un pays à l'autre, notamment en raison du fait que, selon la tradition anglaise, le droit à l'honneur et à la vie privée est de nature strictement personnelle et s'éteint au décès de l'intéressé²⁷.

L'article 9 de la directive sera d'autant plus difficile à mettre en œuvre que la documentation accumulée par les organes des médias vise les personnages publics dont la vie privée est moins intensément protégée que celle des anonymes, sans qu'il soit aisé de circonscrire le « noyau dur » qui devrait être soustrait à toute divulgation.

L'article 9 de la directive est emblématique de la mission impossible assignée au législateur s'il faut par des normes générales concilier les deux libertés que la constitution de stocks de données à caractère personnel mettra nécessairement en conflit. La rigidité de la prévisibilité législative est inapte à embrasser des situations extrêmement diversifiées. D'où l'importance des arbitrages effectués par les autorités indépendantes de protection de la vie privée, grâce à l'adoption de codes de conduite ou de règles directrices (*guidelines*), sous la supervision finale des cours et tribunaux. Dans cette matière, au moins, la toute-puissance de la loi est un dogme dépassé. L'effort de conciliation requis par l'article 9 excède l'exercice traditionnel de la fonction législative : prononcer par voie de dispositions générales.

Droit communautaire et protection des droits de l'homme

Les « règles régissant la liberté d'expression » auxquelles se réfère l'article 9 de la directive appartiennent aussi et, même, au premier chef à un autre ordre juridique. Dans la mise en œuvre de toute la directive, mais spécialement de cet article, les États devront encore veiller au respect de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Sous quelque forme que ce soit, les dispositions qu'ils arrêteront pour donner exécution à la directive seront soumises au contrôle de la Cour européenne des droits de l'homme²⁸, et il existera dès lors deux juridictions internationales compétentes pour vérifier le respect par les États des obligations assumées dans deux ordres juridiques distincts. D'une part, la Cour de justice des Communautés européennes pourra être saisie, par la voie des questions préjudicielles de l'article 177 du traité CE, de toute question d'application ou d'interprétation de la directive et, le cas échéant, de l'action en manquement exercée par la Commission (ou par un autre État) si l'exécution donnée à la directive a été incorrecte ou incomplète. Mais la même exécution pourra aussi faire l'objet d'une requête introduite auprès de la Commission européenne des droits de l'homme²⁹, soit par la personne dont la vie privée aura subi une atteinte en raison de l'action ou de l'omission de l'État, soit par le journaliste, l'artiste, l'écrivain ou l'organe des médias dont la liberté d'expression aurait été injustement brimée. On notera au passage que l'accès direct à la Commission européenne des droits de

²⁶ Voir à titre d'exemple la notice publiée par *The Times*, July 21, 1997, à l'occasion du décès de Sir James Goldsmith.

²⁷ Voir notamment : *Report of the Committee on Privacy and Related Matters*, presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, 1, June 1990, London, HMSO, dit Rapport Calcutt, du nom du président de la Commission, § 7.30 et 7.3 1. Le rapport ne conclut pas à l'opportunité du dépôt d'un projet de loi sur la *privacy* mais il y est annexé un appendice Q, *The Committees Proposed Code of Practice of the Press*, dont le § 16 est rédigé comme suit : « Newspapers should apply the same principles of accuracy, respect for privacy and non-discrimination to stories about the recently-dead as to stories about living ».

²⁸ Tel qu'il sera organisé en vertu du Protocole n° 11 à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, portant restructuration du mécanisme de contrôle établi par la Convention et de l'Annexe 9, faits à Strasbourg le 11 mai 1994. La loi belge du 27 novembre 1996 (*Le Moniteur belge*, 4 juillet 1997, p. 17855) a donné son assentiment à ce Protocole, et l'instrument de ratification a été déposé le 10 janvier 1997. Le Protocole entrera en vigueur le 1^{er} novembre 1997.

²⁹ Cela, jusqu'à l'entrée en vigueur du Protocole n° 11.

l'homme et, ultérieurement, à la Cour est ouvert à toute personne relevant de la compétence d'un État ayant adhéré à la Convention, tandis que les simples particuliers ne peuvent en général soumettre leurs griefs à la Cour de justice des Communautés européennes³⁰.

Sans que l'hypothèse d'un conflit entre les deux juridictions internationales ne puisse être totalement écartée, il est permis d'espérer une coordination des systèmes grâce à la qualification de « principes généraux du droit communautaire » attribuée par la Cour de justice aux dispositions de la Convention européenne et à la valeur interprétative qu'elle reconnaît aux décisions de la Cour européenne des droits de l'homme³¹.

Ayant pour destinataires les États, la directive ne régit pas comme telle le traitement des données à caractère personnel par les organes de la Communauté elle-même. Aussi le traité d'Amsterdam du 2 octobre 1997 a-t-il prévu l'insertion dans le traité CE d'un nouvel article 286 (ex-article 213 B nouveau) rédigé dans les termes suivants :

1. À partir du 1^{er} janvier 1999, 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 institués par le présent traité ou sur la base de celui-ci.
2. Avant la date visée au § 1, le Conseil, statuant conformément à la procédure visée à l'article [189 B], institue un organe indépendant de contrôle chargé de surveiller l'application des dits actes communautaires aux institutions et organes communautaires, et adopte toute autre disposition utile.

VI/ LA DÉTERMINATION DU DOMAINE SPATIAL DU NOUVEAU DROIT DE L'INFORMATIQUE

Qu'elles soient prises en vertu de la directive communautaire, qu'elles aient donné exécution à la Convention européenne du 28 janvier 1981 (dont la nature juridique est similaire à celle de la directive) ou qu'elles suivent les lignes directrices de l'OCDE, les législations nationales sur la protection des données à caractère personnel suscitent trois catégories de problèmes de conflit de lois.

Les législations spécialisées ont énoncé des règles nouvelles soumettant à des obligations administratives les entités et les personnes « responsables » du traitement de telles données, et elles ont institué une autorité publique nouvelle, généralement tenue pour une autorité publique indépendante³². A l'égard de ce premier aspect, le seul problème consiste à déterminer le domaine spatial d'application de cette partie de la loi.

Un second problème concerne le champ d'application des dispositions pénales, soit celles du droit commun, soit les incriminations spéciales prévues par les lois sur la protection des données. Dans les deux cas, et sauf si le législateur en a disposé autrement, il faut appliquer les règles de droit pénal international en vigueur dans l'État dont les tribunaux sont, le cas échéant, saisis d'une infraction.

³⁰ La demande de question préjudicielle est formulée par la juridiction nationale saisie d'un litige auquel une norme de droit communautaire est applicable, les parties à la cause ne pouvant que solliciter une telle mesure. Quant au recours de légalité de l'article 173 du traité CE, il n'est ouvert aux personnes physiques ou morales que dans l'hypothèse très exceptionnelle de l'alinéa 4.

³¹ Sur le difficile problème des rapports entre les deux ordres juridiques, voir notamment : Commission européenne des droits de l'homme, 9 février 1990, *Rev. trim. dr. h.*, 1991, 395, et la note sous Cour européenne des droits de l'homme, 29 novembre 1992, *Rev. trim. dr. h.*, 1993, 335.

³² Voir notamment F. Rigaux, *op. cil.* (n. 3, p. 26), n° 19.

Le traitement automatisé de données à caractère personnel met aussi en jeu des institutions traditionnelles du droit civil interne, notamment, comme on l'a vu, le contrat et la responsabilité. C'est à propos de ces institutions que se pose, dans les termes les plus classiques, un problème de conflit de lois, au sens du choix de la loi applicable à la situation.

La détermination du domaine spatial des lois étatiques conformément à l'article 4 de la directive

L'article 4 de la directive est, pour l'essentiel, resté fidèle au principe de territorialité, encore que ce principe soit d'application délicate à des opérations qu'il est aisé — et qu'il devient de plus en plus aisé — de délocaliser. C'est le lieu du traitement sur le territoire d'un État membre qui fixe le domaine d'application de la législation de cet État. Quand le traitement est réparti entre les établissements que le responsable maintient sur le territoire de plusieurs États membres, ce responsable doit veiller au respect, par chacun des établissements, des obligations prévues par la loi locale (art. 4, al. 1^{er}, a). Comme le précisent les considérants (18) et (19) du préambule, l'harmonisation du droit en vigueur dans les États membres, finalité propre de la directive, a pour conséquence que le responsable du traitement n'a pas le devoir, et l'État sur le territoire duquel se trouve l'établissement principal n'a pas le pouvoir de vérifier selon la loi de cet État si la partie du traitement effectuée sur le territoire d'un autre État membre satisfait aux exigences de la loi du premier État.

Le principe de territorialité fait l'objet d'un rattachement alternatif: quand le responsable du traitement n'est pas établi sur le territoire de la Communauté, l'État membre sur le territoire duquel sont situés « des moyens, automatisés ou non » auxquels il est recouru pour le traitement a le devoir d'y appliquer ses dispositions protectrices (art. 4, al. 1^{er}, c). Dans la même hypothèse, le responsable du traitement « doit désigner un représentant établi sur le territoire dudit État membre » (art. 4, al. 2).

Ce que la directive veut éviter par cette disposition est que des données recueillies sur le territoire d'un État membre puissent être traitées dans un État tiers hors de tout contrôle communautaire. C'est ainsi que le critère justifiant l'application du droit d'un État membre est tantôt le lieu de l'établissement ou des établissements du responsable du traitement, tantôt la localisation des moyens mis en œuvre dans le territoire de cet État par un responsable établi en dehors de la Communauté.

L'article 4, alinéa 1^{er}, b) prévoit un autre critère justifiant l'application de la loi d'un État membre, à savoir la personnalité des lois. Selon le commentaire qu'en donnent Damman et Simitis (n. 1, p. 30), cette disposition viserait les traitements faits par les services diplomatiques d'un État membre sur le territoire d'un autre État membre. Le contrôle en serait soustrait à l'État territorial conformément à la Convention de Vienne sur les relations diplomatiques (p. 128-129).

Le champ d'application des incriminations pénales

L'article 24 de la directive fait une référence peu explicite aux « sanctions » que les États appliquent (et, sans doute, doivent appliquer) « en cas de violation des dispositions prises en application de la présente directive ». Le considérant (21) du préambule n'est guère plus explicite :

(21) considérant que la présente directive ne préjuge pas les règles de territorialité applicables en matière de droit pénal.

À la vérité, le champ d'application du droit pénal n'est pas enfermé dans les « règles de territorialité ». Le principe de territorialité signifie d'abord que les juridictions répressives déterminent leur compétence en vertu des critères posés par la *lex fori* et qu'elles appliquent les incriminations et les peines prévues par la même loi. Toutefois la territorialité n'est pas le seul critère de la compétence pénale : une juridiction répressive peut être compétente en raison de la nationalité soit de l'auteur de l'infraction, soit de la victime. Si un tel délit a été commis à l'étranger, les incriminations et les peines sont déterminées par la *lex fori* sous réserve de la règle de la double incrimination : un fait ne peut être réprimé selon la *lex fori* s'il n'est pas punissable selon le droit du pays où il a été commis. Enfin, surtout à l'égard de comportements aussi difficiles à localiser que les traitements informatisés, le critère de territorialité est d'un maniement difficile et les hypothèses de plurilocalisation ne seront pas rares.

Les conflits de lois en matière de responsabilité civile et de contrat

L'article 23 de la directive impose aux États membres de garantir aux victimes d'un traitement illicite le droit d'obtenir la réparation de leur préjudice sans qu'il soit précisé en vertu de quelle loi pareille responsabilité sera déterminée. Quelques indications peuvent être données sur l'ampleur des problèmes : détermination du lien de causalité, étendue de la réparation, nature du dommage, admission ou non du dommage moral, du dommage émotionnel, du dommage par ricochet, perte du manque à gagner. Face à la diversité des solutions, le choix de la loi applicable revêt toute son importance, mais il n'existe pas non plus, en la matière, de solution commune à tous les États membres. Sans doute l'application de la *lex loci delicti* est-elle assez généralement admise, mais, outre la difficulté de localiser le fait illicite, la règle elle-même s'accompagne d'exceptions et elle peut être évincée en vertu de l'exception d'ordre public. Quant à la localisation du fait, il semble que doive être préféré le rattachement « au lieu où les droits invoqués sont lésés, au domicile (ou à la résidence habituelle) de la victime »³³.

Le choix de la loi applicable au contrat suscitera moins d'hésitation parce que la plupart des États membres de l'Union européenne ont adhéré à la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles. De plus, le droit des contrats n'a pas, dans l'économie de la directive et des méthodes actuelles de protection des données, une incidence aussi étendue que le droit de la responsabilité. Sans doute l'article 7 *b*) de la directive se réfère-t-il au contrat à l'exécution duquel un traitement informatisé est nécessaire, mais il est peu vraisemblable que la validité d'un tel contrat ou son interprétation soulève une question de conflit de lois préalable à l'application de la loi mettant en œuvre cette disposition.

Conclusion

Nul n'ignore que la directive 95/46 est le fruit d'efforts pénibles et soutenus, et il ne faut pas s'étonner que le texte issu de ce long travail pousse à l'extrême l'art de balancer des intérêts contradictoires et de dissimuler sous une phraséologie alambiquée les conflits qui ont divisé les rédacteurs eux-mêmes. Sans doute était-il impossible de faire mieux, mais la marge de manœuvre considérable laissée aux différents législateurs internes et l'impossibilité où se trouveront ceux-ci de fournir une copie beaucoup plus satisfaisante auront pour nécessaire conséquence que

³³ Pierre Bourel, « Du rattachement de quelques délits spéciaux en droit international privé », *Recueil des cours de l'Académie de droit international*, t. 214, p. 255-397, p. 338. Dans le même sens : F. Rigaux, *op. cit.* (n. 3, p. 28), n° 33, p. 472-473.

l'objectif d'harmonisation des droits en vigueur dans les États membres de l'Union européenne ne sera que partiellement atteint.

Force est de constater que la nature radicalement conflictuelle des intérêts mis en jeu par l'informatisation de la société, la diversité des situations manifestant de tels conflits et la volonté de tenir en équilibre des libertés fondamentales antagonistes résistent à l'énoncé de règles dessinant de manière précise et stable les procédés de solution de ces conflits. Mais il faut surtout dissiper la croyance illusoire en la possibilité de maintenir en équilibre les intérêts et les valeurs qui se font face. La justice ne manie pas une balance dont le fléau se tient de manière permanente en position horizontale. L'œuvre de justice consiste inéluctablement à faire pencher un des plateaux vers le bas et à hisser l'autre vers le haut. Selon les données et les circonstances propres à chaque espèce ou communes à une catégorie d'espèces³⁴, c'est tantôt une liberté tantôt l'autre qui l'emporte, et cette œuvre de justice ne saurait être accomplie par un législateur, et moins que tout par un instrument tenu de concilier les traditions juridiques d'un nombre croissant d'États³⁵. Cela rend d'autant plus importante la fonction des autorités publiques investies du pouvoir de contrôler le respect effectif de principes formulés en termes nécessairement généraux et souvent ambigus. Et à la fin du jour il appartiendra aux tribunaux étatiques, aux juridictions constitutionnelles et aux deux Cours européennes de donner une consistance passagère aux mêmes principes et de vider les conflits qui les opposent les uns aux autres.

³⁴ On aura reconnu la distinction entre deux méthodes de pondération des intérêts, le *categorical balancing* et l'*ad hoc balancing* (*Abägung im Einzelfall*).

³⁵ Voir notamment: Pierre Legrand, « European Legal Systems are not converging », 45, ICLQ (1996), 52-81, et comp. plusieurs contributions de l'ouvrage collectif: *The Common Law of Europe and the Future of Legal Education*, ed. by Bruno De Witte and Caroline Forder (Metro, Kluwer, 1992).