



Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

(STE n° 108)

English

Rapport explicatif

I. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, élaborée au sein du Conseil de l'Europe par un comité d'experts gouvernementaux sous l'autorité du Comité européen de coopération juridique (CDCJ), a été ouverte à la signature des Etats membres du Conseil de l'Europe le 28 janvier 1981 à Strasbourg, à l'occasion de la troisième partie de la 32e Session de l'Assemblée Consultative.

II. Le texte du rapport explicatif préparé par le comité d'experts et soumis au Comité des Ministres tel qu'amendé par le CDCJ ne constitue pas un instrument d'interprétation authentique du texte de la Convention, bien qu'il puisse faciliter la compréhension des dispositions qui y sont contenues.

Introduction

Protection des données

1. La présente Convention a pour objet de renforcer la protection des données, c'est-à-dire la protection juridique des individus vis-à-vis du traitement automatisé des données à caractère personnel les concernant.

Ce renforcement est rendu nécessaire par l'utilisation croissante de l'informatique à des fins administratives et de gestion. Les fichiers automatisés ont une capacité d'enregistrement bien supérieure à celle des fichiers manuels et permettent de procéder très rapidement à des opérations beaucoup plus variées.

Au cours des années à venir, le traitement automatisé des informations continuera à s'imposer dans le domaine administratif et de gestion et cela notamment en raison de l'abaissement des coûts du traitement informatique des données, de l'apparition sur le marché de dispositifs de traitement «intelligents» et de la mise en place de nouveaux équipements de télécommunications pour la transmission des données.

2. Le «pouvoir de l'informatique» fait peser une responsabilité sociale correspondante sur les utilisateurs dans les secteurs privé et public. Dans la société moderne, une grande partie des décisions affectant les individus

reposent sur des données enregistrées dans des fichiers informatisés: feuilles de paie, dossiers de sécurité sociale, dossiers médicaux, etc. Il est essentiel que les responsables de ces fichiers s'assurent que les avantages indéniables qu'ils peuvent obtenir du traitement automatisé des données n'aboutissent, en même temps, à affaiblir la position des personnes concernées par les données enregistrées. Pour cette raison ils devraient veiller à la bonne qualité des informations qui leur sont confiées, s'abstenir d'enregistrer des informations qui ne sont pas nécessaires à la poursuite de la finalité déclarée, se garder de diffuser des informations sans autorisation ou d'en abuser, et protéger les données, le matériel et le logiciel, de tout risque d'endommagement.

3. Les systèmes juridiques des Etats membres ne sont pas entièrement dépourvus de règles tendant à cette fin. On y trouve par exemple des lois sur la vie privée, sur la responsabilité civile, sur le secret ou la confidentialité d'informations sensibles, etc. Toutefois, on manque de règles générales sur l'enregistrement et l'utilisation d'informations à caractère personnel et, en particulier, sur le point de savoir comment permettre aux individus d'exercer un contrôle sur les informations les concernant que d'autres rassemblent et utilisent.

Action du Conseil de l'Europe

4. En 1968, l'Assemblée parlementaire du Conseil de l'Europe avait adressé au Comité des Ministres sa Recommandation 509 dans laquelle elle lui demandait de déterminer si la Convention européenne des Droits de l'Homme et les législations internes des Etats membres suffisaient à protéger le droit à la vie privée face à la science et à la technologie modernes.

Pour donner suite à cette recommandation, le Comité des Ministres a fait entreprendre une étude dont les résultats ont révélé que les législations nationales actuelles offraient une protection insuffisante à la vie privée ainsi qu'aux autres droits et intérêts des personnes physiques vis-à-vis des banques de données automatisées.

Se fondant sur cette constatation, le Comité des Ministres a adopté en 1973 et 1974 deux résolutions concernant la protection des données. La première de ces résolutions, la Résolution (73) 22, énonçait les principes de la protection des données pour le secteur privé, la seconde, la Résolution (74) 29, a fait de même pour le secteur public.

Législation nationale

5. Ces deux résolutions énumèrent les règles fondamentales à observer en cas d'enregistrement d'informations à caractère personnel dans les banques de données électroniques. Bien qu'elles aient laissé aux Etats membres toute latitude pour déterminer comment donner effet à ces règles, on constate que la quasi-totalité desdits Etats ont décidé ou envisagé de le faire par la voie législative.

Au cours des cinq années qui ont suivi l'adoption de la seconde résolution, des lois générales sur la protection des données étaient promulguées dans sept Etats membres (Autriche, Danemark, France, République Fédérale d'Allemagne, Luxembourg, Norvège et Suède). Dans trois Etats membres la protection des données figure en tant que droit fondamental dans la

Constitution (article 35 de la Constitution du Portugal de 1976; article 18 de la Constitution de l'Espagne de 1978; article 1 de la loi autrichienne sur la protection des données de 1978: droit fondamental de la protection des données).

L'Assemblée Parlementaire du Conseil de l'Europe, tenant compte de cette dernière tendance, a recommandé au Comité des Ministres dans sa Recommandation 890 (1980), d'étudier l'opportunité d'insérer dans la Convention des Droits de l'Homme une disposition sur la protection des données.

Dans plusieurs autres Etats membres (notamment la Belgique, l'Islande, les Pays-Bas, l'Espagne et la Suisse), une législation sur la protection des données se trouve à un stade de préparation avancé.

6. Les grandes lignes de ces législations sont conformes aux principes établis dans les Résolutions (73) 22 et (74) 29 du Comité des Ministres. Toutes les lois nationales sur la protection des données ainsi que les propositions de législation qui ont été rendues publiques contiennent des règles similaires sur le droit matériel relatif au traitement des données, c'est-à-dire sur la qualité des données et sur leur utilisation.

Bien que les règles de procédure diffèrent d'un pays à l'autre suivant leur système juridique général, on trouve un large accord sur les buts que ces règles doivent atteindre. Toutes les lois nationales reconnaissent: i. le principe de la publicité, c'est-à-dire que l'existence de fichiers automatisés de données soit portée à la connaissance du public, et ii. le principe du contrôle, c'est-à-dire que les autorités publiques de surveillance ainsi que les individus directement concernés par les informations puissent prétendre à ce que les droits et intérêts de ces individus soient respectés par les utilisateurs.

7. Dans la plupart des pays, la loi sur la protection des données a ou aura une large portée en s'appliquant au traitement des données aussi bien dans le secteur public que dans le secteur privé. Dans certains Etats, en outre, son champ d'application couvre non seulement les fichiers automatisés mais également certaines catégories de fichiers manuels. Dans tous les pays, elle s'applique aux données relatives aux personnes physiques, tandis que dans certains Etats elle couvre également des données concernant les personnes morales. Lorsque, pour des raisons d'intérêt public, certaines restrictions ou exceptions aux règles générales sont nécessaires, elles sont généralement prévues par la loi elle-même.

Flux transfrontières de données à caractère personnel

8. La question s'est posée de savoir dans quelle mesure les lois nationales sur la protection des données offrent une protection adéquate aux individus lorsque les informations les concernant font l'objet de flux transfrontières. Les ordinateurs, associés aux télécommunications, sont en train d'ouvrir de nouvelles perspectives pour le traitement des données au plan international. Ils aident à surmonter plusieurs types de barrières qui font obstacle à la communication entre les nations: distance, temps, langue et coût. Le traitement dispersé permet aux utilisateurs de répartir un système d'information ou une base de données sur plusieurs pays. Les réseaux permettent aux utilisateurs d'accéder où de relier des systèmes d'information situés dans des pays éloignés. Dans plusieurs secteurs (par

exemple banques, voyages, cartes de crédit, etc.), de telles applications de traitement transfrontières des données sont désormais courantes

9. Qu'il s'agisse des utilisateurs ou des personnes concernées il ne devrait pas être fait de différence selon que les opérations de traitement s'effectuent dans un ou plusieurs pays. Les mêmes règles fondamentales devraient s'appliquer et les personnes concernées devraient avoir les mêmes garanties pour la protection de leurs droits et intérêts.

En pratique toutefois la protection des personnes perd en efficacité lorsque l'aire géographique s'élargit. On craint notamment que les utilisateurs ne soient tentés d'éviter les contrôles imposés par la protection des données en déplaçant leurs opérations, en totalité ou en partie, vers des «paradis de données», c'est-à-dire dans des pays ayant des lois sur la protection des données moins strictes, voire sans lois.

Afin de pallier ce risque, certains Etats ont institué dans leur droit interne des contrôles spéciaux sous forme, par exemple, d'autorisations d'exportation.

Cependant de tels contrôles pourraient entraver la libre circulation internationale des informations qui constitue un principe d'importance fondamentale tant pour les individus que pour les peuples. Une formule devait donc être trouvée afin de garantir que la protection des données au plan international ne porte pas préjudice à ce principe.

Nécessité d'un accord international

10. Même parmi des Etats qui ont un système de loi sur la protection des données très similaire, des problèmes se posent tant par rapport à la loi elle-même que pour son application pratique. Lorsque le traitement automatisé de données à caractère personnel met en jeu des parties dans différents pays (dans le cas par exemple d'une banque de données dans un pays reliée à des terminaux dans d'autres pays), il est parfois difficile de déterminer quel Etat a juridiction et quelle loi nationale est applicable.

En outre, des personnes résidant dans un pays peuvent rencontrer des difficultés lorsqu'elles veulent exercer leurs droits à l'égard de fichiers automatisés situés dans d'autres pays. De tels problèmes ne peuvent être résolus d'une façon satisfaisante que par une coopération internationale.

11. Plus généralement, tenant compte de l'évolution rapide des techniques de traitement des informations et du développement de la circulation internationale des données, il est souhaitable de créer des mécanismes au niveau international, permettant aux Etats de se tenir informés et de se consulter en matière de protection des données.

Mandat pour la Convention

12. En 1972, lorsqu'un comité d'experts préparait les résolutions sur la protection des données (cf. paragraphe 5), il avait souligné que la prochaine étape après la promulgation de législations nationales fondées sur ces résolutions devait être le renforcement de ces règles nationales au moyen d'un accord international contraignant. Telle fut d'ailleurs la proposition de la 7e Conférence des ministres européens de la justice (Bale 1972) dans sa Résolution n° 3.

Le comité avait pris en considération deux modèles pour un tel accord. Le premier se fondait sur la réciprocité: un Etat ne devrait pas permettre sur son territoire des opérations de traitement concernant des personnes résidant dans un autre Etat, si de telles opérations étaient illégales aux termes des lois de ce dernier Etat.

Ce modèle se fondait sur l'hypothèse que chaque Etat appliquerait ses propres critères de protection des données. Outre les complications pratiques qu'il comportait, ce modèle était contraire à l'idée que toute personne devrait jouir, à la base, des mêmes droits. Le comité avait en conséquence préféré un second modèle, fondé sur des principes de protection des données communs à toutes les Parties.

13. En 1976, le Comité des Ministres a chargé le Comité d'experts sur la protection des données, dépendant du Comité européen de coopération juridique (CDCJ), «d'élaborer une Convention pour la protection de la vie privée par rapport au traitement des données à l'étranger et au traitement transfrontière des données» (Activité n° 21.20.1 du programme d'activités intergouvernementales).

Coopération avec l'OCDE et la CEE

14. Le comité a été chargé de s'acquitter de cette tâche en étroite collaboration avec l'Organisation de coopération et de développement économiques, ainsi qu'avec les Etats non européens membres de cette Organisation, en tenant compte des activités menées par l'OCDE dans le domaine de la politique de l'information, de l'informatique et des communications. Une liaison étroite a été maintenue entre les deux Organisations, au niveau du Secrétariat comme à celui du comité d'experts du Conseil de l'Europe et du comité correspondant de l'OCDE, le Groupe sur les banques de données auquel avait succédé en 1978 un Groupe d'experts sur les obstacles au mouvement transfrontière des données. Ce dernier groupe fut chargé par le Conseil de l'OCDE d'élaborer des lignes directrices sur la protection de la vie privée en vue de faciliter l'harmonisation des législations nationales des Etats membres de l'OCDE, sans préjuger de la possibilité d'établir, à un stade ultérieur, une convention internationale.

15. L'OCDE ainsi que quatre de ses Etats membres non européens (Australie, Canada, Japon et Etats-Unis) ont été représentés par un observateur au sein du comité du Conseil de l'Europe. Des observateurs de la Finlande, de la Conférence de La Haye de droit international privé et des Communautés européennes prirent également part aux travaux.

16. La Commission des Communautés européennes, qui a effectué des études sur l'harmonisation des législations nationales dans le cadre de la Communauté par rapport aux flux transfrontières des données et sur les distorsions de concurrence éventuelles, ainsi que sur les problèmes liés à la sécurité des données, a maintenu des contacts étroits avec le Conseil de l'Europe. La Commission a décidé d'attendre l'issue des travaux concernant la présente Convention avant de prendre position sur sa propre action en matière de protection des données. Le Parlement européen a également manifesté un vif intérêt pour la protection des données. Lors de sa session de mai 1979, il a adopté une Résolution sur la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique et il l'a communiquée au Comité des Ministres du Conseil de l'Europe.

Travaux du Comité d'experts sur la protection des données

17. De novembre 1976 à mai 1979, le Comité d'experts sur la protection des données a tenu quatre réunions, d'abord sous la présidence de M. L. Joinet (France), puis sous celle de M. R.A. Harrington (Royaume-Uni). Un groupe de travail composé d'experts de l'Autriche, de la Belgique, de la France, de la République Fédérale d'Allemagne, de l'Italie, des Pays-Bas, de l'Espagne, de la Suède, de la Suisse et du Royaume-Uni, s'est réuni à plusieurs reprises entre les sessions du comité plénier pour approfondir l'économie générale et les détails du projet de Convention.

En avril 1980 un nouveau comité d'experts, présidé par M. J. Voyame (Suisse), a révisé et mis au point le texte. Celui-ci a été approuvé par le CDCJ à sa 33^e réunion et adopté par le Comité des Ministres qui a décidé de l'ouvrir à la signature le 28 janvier 1981.

Traits principaux de la Convention

18. La Convention se compose de trois parties principales:

- dispositions de droit matériel sous forme de principes de base;
- règles spéciales concernant les flux transfrontières de données;
- mécanismes d'entraide et de consultation entre les Parties.

19. 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 (cf. article 10 de la Convention européenne des Droits de l'Homme; article 19 du Pacte international sur les droits civils et politiques). Lorsque la présente Convention prévoit des restrictions ou conditions à l'exercice de la liberté d'information, ce n'est que dans la mesure où cela est strictement justifié par la protection d'autres droits et libertés individuels, notamment le droit au respect de la vie privée (cf. article 8, Convention européenne des Droits de l'Homme).

Toutefois, il n'a pas paru souhaitable de se baser exclusivement sur la Convention européenne des Droits de l'Homme pour ce qui est de la protection des données, notamment parce que cette Convention est un instrument «fermé», qui ne permet pas la participation d'Etats non-membres et non européens.

20. La partie centrale du projet de Convention est le chapitre II qui contient les principes de base pour la protection des données. Chaque Partie devrait prendre les mesures nécessaires pour donner suite à ce «noyau dur» dans sa législation interne. Le préluce à ces dispositions se trouve dans les principes énoncés auparavant dans les Résolutions (73) 22 et (74) 29 du Comité des Ministres, ces derniers ayant été complétés, lorsque cela s'est avéré approprié, à la lumière des développements ultérieurs dans les Etats membres.

Il y a lieu de noter que la Convention donne des indications claires et précises sur l'objectif à atteindre par chaque principe, tout en laissant à chaque Partie le soin de déterminer la manière de le mettre en œuvre dans son droit interne.

Les principes du «noyau dur» reconnaissent aux personnes concernées dans tous les Etats où la Convention s'applique, un certain minimum de protection au regard du traitement automatisé de données à caractère personnel. En s'engageant à appliquer ces principes, les Parties tendent à supprimer entre elles les restrictions aux flux transfrontières de données, évitant ainsi que le principe de libre circulation des informations soit mis en cause par des formes de protectionnisme. En outre, le «noyau dur» aboutira à une harmonisation des lois entre les Parties et, par conséquent, comportera une diminution des possibilités de conflits de lois ou de juridiction.

21. Le chapitre III concernant les flux transfrontières de données vise à concilier les exigences simultanées et parfois concurrentes de la libre circulation des informations et de la protection des données, la règle fondamentale étant que les flux transfrontières de données entre Parties ne devraient pas être assujettis à un contrôle spécial. Cette disposition devrait être regardée en étroite liaison avec le chapitre II qui garantit que le traitement de données à caractère personnel est soumis, dans tous les pays concernés, aux mêmes règles fondamentales («noyau dur»).

22. Les chapitres IV et V prévoient les mécanismes de coopération entre les Parties, tant dans des cas concrets (chapitre IV: assistance mutuelle entre autorités et assistance aux personnes concernées à l'étranger), qu'au regard de la Convention dans son ensemble (chapitre V).

La formule retenue permet de restreindre le contenu de la Convention aux principes de base et de s'en remettre à la coopération entre les Etats, dans le cadre d'un Comité consultatif, pour la mise en œuvre et l'harmonisation de ces principes dans leur droit interne.

23. Le comité d'experts s'est également penché sur la question de savoir si la Convention devait contenir des règles pour résoudre des problèmes de loi applicable. De tels problèmes peuvent se poser lorsque des opérations de traitement de données sont effectuées sur le territoire de deux ou plusieurs Etats (contractants ou non contractants) ou lorsque les sujets concernés par le traitement des données, notamment les personnes ou les utilisateurs des fichiers résident dans des pays différents. Le comité a décidé qu'il était prématuré d'inclure dans la Convention des règles spécifiques sur ce sujet. La présence d'un «noyau dur» de droit matériel (chapitre II), y compris certains principes de procédure, permettront de réduire le risque de conflits de lois ou les lacunes juridiques. Le comité était convenu, cependant, que le problème de la loi applicable serait gardé à l'esprit et que, à un stade ultérieur, des dispositions sur ce sujet seraient - si nécessaire - établies dans un Protocole à la Convention.

Commentaires sur les dispositions de la Convention

Titre

24. Le titre décrit cet instrument comme «Convention», et non «Convention européenne» afin de mieux souligner qu'elle doit se prêter à l'adhésion d'Etats non européens.

Préambule

25. Le préambule réaffirme l'engagement des Etats signataires en faveur des droits de l'homme et des libertés fondamentales. Il admet, en outre, que dans certaines conditions, l'exercice d'une complète liberté de traiter les informations risque de nuire à la jouissance d'autres droits fondamentaux (par exemple les droits à la vie privée, à la non-discrimination et à un procès équitable) ou à d'autres intérêts personnels légitimes (par exemple en matière d'emploi ou de crédit à la consommation). C'est pour maintenir un juste équilibre entre les différents droits et intérêts des personnes que la Convention impose certaines conditions ou restrictions au traitement d'informations. Aucun autre motif ne saurait justifier les règles que les Etats contractants s'engagent à appliquer dans ce domaine.

Il est souligné également que la Convention ne doit pas être interprétée comme un moyen d'ériger des barrières non tarifaires au commerce international ou de restreindre les échanges d'informations scientifiques et culturelles.

Chapitre 1 – Dispositions générales

Article 1 – Objet et but

26. Le premier article est consacré à une description de l'objet et du but de la Convention.

Les garanties énoncées dans la Convention s'étendent à toute personne physique, indépendamment de sa nationalité ou de son lieu de résidence. Cette disposition est conforme au principe général observé par le Conseil de l'Europe et ses Etats membres en faveur de la protection des droits individuels. Des clauses restreignant la protection des données aux ressortissants d'un Etat ou aux étrangers résidant légalement sur son territoire sont donc incompatibles avec la Convention.

Article 2 – Définitions

27. Les définitions figurant dans la présente Convention sont conçues pour s'appliquer, le cas échéant, à différents termes ou expressions traduisant certains concepts fondamentaux dans les législations nationales. Les termes et définitions utilisés sont le plus souvent identiques à ceux des Résolutions (73) 22 et (74) 29. Il a été procédé à certaines modifications et additions afin de tenir compte des lois promulguées récemment dans les pays membres et des problèmes particuliers que soulèvent les flux transfrontières de données.

Littera a

28. «Personne identifiable» s'entend d'une personne qui peut être facilement identifiée; cela ne couvre pas l'identification de personnes par des méthodes très complexes.

29. La notion de «personne concernée» exprime l'idée selon laquelle toute personne possède un droit subjectif par rapport aux informations qui la concernent, même si ces informations sont rassemblées par d'autres (cf. l'expression *data subject* en anglais).

Littera b

30. La définition 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 traitement.

L'expression «fichier automatisé» a remplacé celle de «banque de données électronique», utilisée auparavant dans les Résolutions (73) 22 et (74) 29, ainsi que dans certaines lois nationales. Aujourd'hui «banque de données» est utilisé dans un sens plus spécialisé, notamment: un fond commun de données accessible à plusieurs utilisateurs.

Littera c

31. Sous réserve des dispositions des articles 5.a et 12, la collecte d'informations ne rentre pas dans la notion de «traitement».

En raison de l'évolution rapide de la technologie du traitement des données, il a été jugé opportun de donner du «traitement automatisé» une définition assez générale et susceptible d'une interprétation flexible.

«Diffusion» est un terme large couvrant tant la divulgation d'informations à une personne (ou à plusieurs personnes) que la consultation des informations par ces personnes.

Littera d

32. En ce qui concerne l'expression «maître du fichier», il y a lieu de signaler que la Convention vise exclusivement la personne ou l'organe responsable en dernier ressort du fichier et non pas les personnes qui procèdent aux opérations de traitement conformément aux instructions du maître du fichier.

La référence à la «loi nationale» tient compte du fait que les différentes lois sur la protection des données contiennent des critères précis pour l'identification de la personne compétente.

Aux termes de l'article 8.a. il devrait toujours être possible de découvrir l'identité du maître du fichier.

Article 3 – Champ d'application

33. Conformément au *paragraphe 1*, la Convention s'applique aux secteurs public et privé. Bien que la plus grande partie de la circulation internationale des données concerne le secteur privé, la Convention revêt une grande importance pour le secteur public et ceci pour deux raisons: tout d'abord, l'article 3 impose l'obligation aux Etats membres d'appliquer les principes de protection des données même s'ils traitent des fichiers publics - comme c'est généralement le cas - entièrement à l'intérieur de leurs frontières nationales. Ensuite, la Convention offre assistance aux personnes concernées qui souhaitent exercer leur droit d'être informées sur leur dossier détenu par une autorité publique dans un pays étranger.

La distinction secteur public/secteur privé ne se retrouve pas dans les autres dispositions de la Convention, notamment parce que ces notions peuvent avoir une signification différente d'un pays à l'autre. Mais elle peut

jouer un rôle dans les déclarations que les Parties ont la faculté de faire pour ce qui est du champ d'application de la Convention (paragraphe 2).

34. *Paragraphe 2.a.* Il est à souligner que des exclusions au champ d'application de la Convention ne seront permises qu'à l'égard de catégories de fichiers qui ne sont pas, ou pas encore, assujetties à une législation interne en matière de protection des données.

En ce qui concerne les catégories de fichiers déjà incluses dans cette législation, des dérogations ne seront possibles qu'en vertu de l'article 9.

35. Il est entendu que toute exception doit être clairement précisée afin d'éviter que les autres Etats contractants ne rencontrent des difficultés quant à l'interprétation de l'exception, ce qui pourrait gravement entraver l'application de la Convention.

36. *Paragraphe 2.b et c.* Ces paragraphes permettent aux Etats d'étendre la protection prévue par la Convention à des personnes concernées qui ne sont pas des personnes physiques, ainsi qu'aux fichiers manuels. Ces Etats peuvent invoquer la règle de la réciprocité à l'égard d'Etats qui n'ont pas fait de telles extensions (paragraphe 4).

37. Le *paragraphe 5* détermine le moment de la prise d'effet des déclarations prévues dans cet article, ainsi que la procédure à suivre pour leur retrait.

Chapitre II – Principes de base pour la protection des données

Article 4 – Engagement des Parties

38. Comme cet article l'indique, la Convention oblige les Parties à incorporer des dispositions sur la protection des données dans leur législation. En effet, la Convention n'a pas été conçue comme *self executing* et par conséquent les droits des individus ne peuvent découler directement d'elle.

39. En fonction du système juridique et constitutionnel du pays concerné, les «mesures nécessaires dans son droit interne» peuvent revêtir, outre la loi, différentes formes telles que règlements, directives administratives, etc. De telles mesures contraignantes peuvent utilement être complétées par des mesures de réglementation volontaire dans le domaine de l'informatique, telles que des codes de bonne pratique ou des règles de conduite professionnelle. Toutefois ces mesures volontaires ne suffisent pas par elles-mêmes pour donner suite à la Convention.

Il est stipulé en outre que les mesures nécessaires pour donner suite à la Convention doivent être en place au moment où la Convention prend effet à l'égard du pays concerné afin d'éviter qu'il ne se crée un hiatus entre la date de l'entrée en vigueur de la Convention et celle de l'introduction de ses mesures dans le droit interne. Lorsque, pour des raisons légitimes, le droit interne ne s'applique pas encore à telle ou telle catégorie de fichiers, il y a lieu de faire une exclusion aux termes de l'article 3.a.

Article 5 – Qualité des données

40. Les dispositions de cet article correspondent largement aux principes énoncés dans les Résolutions (73) 22 et (74) 29 et peuvent également être retrouvées, dans des termes quasi similaires, dans les lois nationales sur la protection des données promulguées avant la Convention.

Deux règles principales sont exprimées par les différentes dispositions de cet article. D'une part l'information elle-même doit être correcte, pertinente et non excessive par rapport à sa finalité. D'autre part, son utilisation (collecte, enregistrement, diffusion) doit également être correcte.

41. La référence aux «finalités» dans les lettres b et c indique qu'il ne sera pas permis d'enregistrer des données pour des finalités non déterminées. La façon dans laquelle la finalité légitime est précisée peut varier selon le droit interne.

42. L'exigence figurant sous la lettre e concernant la durée limitée de la conservation des données sous leur forme nominative ne signifie pas qu'elles doivent être séparées, après quelque temps, irrévocablement du nom de la personne à laquelle elles se réfèrent, mais seulement qu'il ne doit pas être possible de relier facilement les données et les identifiants.

Article 6 – Catégories particulières de données

43. Bien que le risque pour les personnes, présenté par le traitement des données, dépende en principe non pas du contenu des données elles-mêmes mais du contexte dans lequel elles sont utilisées, il y a des cas exceptionnels où le traitement de certaines catégories de données peut, en tant que tel, porter préjudice aux droits et intérêts des individus. Cet article énumère quelques catégories de données qui dans tous les Etats membres sont considérées comme étant particulièrement sensibles.

44. L'expression «révélant... les opinions. . . , les convictions ...» couvre également les activités découlant de ces opinions ou convictions.

45. La signification de la notion de «données à caractère personnel relatives à la santé» a été soigneusement étudiée par le Comité d'experts sur la protection des données dans le contexte de ses travaux sur les banques de données médicales. Elle couvre les informations concernant la santé passée, actuelle et future, physique ou mentale d'un individu. Il peut s'agir d'informations sur un individu bien portant, malade ou décédé. Il est entendu que cette catégorie de données comprend également les informations relatives à l'abus d'alcool ou à la consommation de drogues.

46. A l'instar de l'article 4 (paragraphe 39 ci-dessus) l'expression «droit interne» peut être entendue dans un sens large incluant des mesures appropriées et spécifiques non seulement de caractère législatif mais aussi réglementaire ou administratif, à condition que le degré de protection nécessaire soit assuré.

47. Par «condamnations pénales» il y a lieu d'entendre: des condamnations fondées sur une loi pénale et dans le cadre d'une procédure pénale.

48. La liste que contient cet article ne doit pas être considérée comme exhaustive. Un Etat contractant peut en effet, en conformité avec l'article 11, interdire ou restreindre dans sa législation interne le traitement d'autres catégories de données. Le degré de sensibilité des catégories de données

dépend du contexte juridique et sociologique du pays concerné. Par exemple, les informations sur l'appartenance syndicale sont considérées dans un pays comme entraînant des risques pour la vie privée, alors que dans d'autres pays elles ne sont considérées comme sensibles que dans la mesure où elles sont étroitement liées aux opinions politiques.

Article 7 – Sécurité des données

49. Des mesures spécifiques de sécurité devraient être prises pour chaque fichier en fonction de sa vulnérabilité, de la nécessité d'en restreindre l'accès dans le cadre de l'organisation, des impératifs d'un enregistrement à long terme, etc. Les mesures de sécurité doivent être appropriées, c'est-à-dire adaptées aux fonctions spécifiques du fichier et proportionnées aux risques encourus. Enfin, elles doivent être fondées sur l'état actuel des connaissances relatives aux méthodes et techniques de sécurité dans le domaine de l'informatique.

Article 8 – Garanties complémentaires pour la personne concernée

50. Les dispositions énoncées dans cet article sont conçues pour permettre à toute personne concernée de défendre ses droits vis-à-vis des fichiers automatisés. Bien que dans la législation interne le contenu de l'article 8 corresponde clairement à des droits subjectifs, il est libellé sous forme de garanties que les Parties offrent aux personnes concernées, en raison du caractère *non-self executing* de la Convention. Ces garanties comportent quatre éléments principaux:

- connaissance de l'existence d'un fichier automatisé;
- connaissance de la teneur de l'information qu'un fichier contient éventuellement sur le compte de la personne concernée;
- rectification d'une information erronée ou inappropriée;
- un droit de recours si l'un des éléments précédents n'est pas respecté.

51. Pour garantir l'exercice de ces droits, la Convention exige que soit indiqué clairement le nom ou la raison sociale du maître de chaque fichier (lettre a). Le libelle de cet alinéa tient compte de la variété des règles de droit interne donnant effet à ce principe. Dans certains Etats, le nom du maître du fichier est inscrit dans un répertoire public. Dans d'autres Etats n'ayant pas un tel système de publicité, la loi pourra prévoir que le nom du maître du fichier sera communiqué à la personne qui le demandera.

52. Dans les lettres b et c, il n'est pas précisé de la part de qui une personne concernée peut obtenir la confirmation, communication, rectification, etc. Dans la plupart des Etats, il s'agit du maître du fichier, mais dans un certain nombre d'Etats ce droit est réalisé par l'intermédiaire de l'autorité de surveillance.

53. Le libellé de la lettre b est destiné à couvrir les différentes hypothèses suivies par les législations nationales: communication à la demande de l'intéressé ou à l'initiative du maître du fichier; communication gratuite à des intervalles fixes, ainsi que communication payante à toute autre

occasion, etc. Le terme «frais» désigne la redevance qu'on réclame à l'intéressé et non pas le coût réel de l'opération concernée.

54. Lorsque des rectifications sont obtenues en conformité avec le principe énoncé à la lettre c, la loi ou la pratique nationales prévoient généralement que dans des cas appropriés ces rectifications sont communiquées aux destinataires de l'information originale.

Article 9 – Exceptions et restrictions

55. Les exceptions aux principes de base pour la protection des données sont limitées à celles nécessaires pour la protection des valeurs fondamentales dans une société démocratique. Le texte du deuxième paragraphe de cet article a été inspiré par celui des deuxièmes paragraphes des articles 6, 8, 10 et 11 de la Convention européenne des Droits de l'Homme. Il ressort des décisions de la Commission et de la Cour des Droits de l'Homme concernant la notion de «mesure nécessaire» que les critères pour une telle notion ne peuvent pas être fixés pour tous les pays et tous les temps, mais qu'il y a lieu de les considérer par rapport à une situation donnée de chaque pays.

56. La lettre a *du paragraphe 2* énumère les intérêts majeurs de l'Etat qui peuvent exiger des exceptions. Ces exceptions ont été formulées de façon très précise pour éviter qu'en ce qui concerne l'application générale de la Convention les Etats aient une marge de manœuvre trop large.

Les Etats conservent, aux termes de l'article 16, la faculté de refuser l'application de la Convention dans des cas individuels pour des motifs majeurs y compris ceux énumérés à l'article 9.

La notion de «sécurité de l'Etat» doit être entendue dans le sens traditionnel de protection de sa souveraineté nationale contre des menaces tant internes qu'externes y compris la protection des relations internationales de l'Etat.

57. L'expression «intérêts monétaires de l'Etat» comprend tout ce qui concourt à fournir à l'Etat les moyens financiers de sa politique. En ce sens, cette expression se réfère notamment aux exigences du recouvrement de l'impôt ainsi qu'au contrôle des changes. La notion de «répression des infractions pénales» contenue dans cette lettre couvre les enquêtes criminelles ainsi que les poursuites pénales.

58. La lettre b vise les intérêts majeurs des parties privées, ceux de la personne concernée elle-même (par exemple informations psychiatriques) ou des tiers (liberté de la presse, secrets de commerce, etc.).

59. Le *paragraphe 3* prévoit la possibilité de restreindre les droits des personnes concernées dans le cas de traitements ne présentant aucun risque. Un exemple est celui de l'utilisation de données à des fins statistiques, dans la mesure où il s'agit de données présentées sous une forme agrégée et séparées des identifiants. De même la recherche scientifique est mentionnée dans cette rubrique, conformément à une recommandation de la Fondation européenne de la science.

Article 10 – Sanctions et recours

60. Afin que cette Convention puisse garantir une protection des données efficace, les devoirs des utilisateurs et les droits des personnes concernées devraient être assortis dans la législation nationale des Etats membres de sanctions et recours correspondants.

Suivant le caractère *non-self executing* de la Convention, il devrait être laissé aux Etats de déterminer la nature de ces sanctions et recours (civils, administratifs, pénaux).

Article 11 – Protection plus étendue

61. Cet article a été inspiré d'une disposition similaire, l'article 60 de la Convention européenne des Droits de l'Homme. La Convention confirme les principes du droit de la protection des données que toutes les Parties sont prêtes à adopter. Dans le texte il est souligné que ces principes ne constituent qu'une base sur laquelle les Etats peuvent construire un système plus avancé de protection.

Chapitre III – Flux transfrontières de données

Article 12

62. Le but de cet article est de concilier les conditions nécessaires à une protection des données efficace avec le principe de la libre circulation des informations sans considération de frontières, qui est consacré par l'article 10 de la Convention européenne des Droits de l'Homme.

63. La rédaction du *paragraphe 1*, spécifiant la portée de la notion de flux transfrontières des données, tient compte de la grande diversité des facteurs déterminant la façon dont sont transférées les données: leur mode de présentation (texte clair ou encodé); leur support (papier, carte perforée, bande perforée, bande magnétique, disque, etc.), moyen de transport (transport physique, poste, liaison de télécommunications commutée par circuits ou par paquets); interface (ordinateur à terminal, ordinateur à ordinateur, manuel à ordinateur, etc.); circuit emprunté (directement du pays d'origine vers le pays de destination, ou via un ou plusieurs pays de transit); relations entre expéditeur et destinataire (appartenant à une même ou à différentes organisations), etc.

64. Aux termes du *paragraphe 1*, les dispositions de l'article 12 s'appliquent également à la collecte de données. Cette extension a été jugée indispensable afin d'éviter que des données rassemblées dans un pays et traitées dans un autre n'échappent aux normes indiquées par cette Convention.

65. Dans ce *paragraphe* il est établi avec clarté que les dispositions de l'article 12 ne s'appliquent qu'aux flux transfrontières de données à caractère personnel. Il est toutefois entendu que si deux ou plusieurs Etats contractants, en se prévalant de la faculté prévue à l'article 3, *paragraphe 2.b*, ont déclaré appliquer la Convention à des informations afférentes aux personnes morales, l'article 12, comme d'ailleurs les autres articles de la Convention, s'appliquera à de telles informations mais exclusivement entre les Etats qui ont fait cette déclaration. Par contre, un Etat contractant qui a exclu du champ d'application de la Convention certaines catégories de données aux termes de l'article 3, *paragraphe 2.a* sera, en fait, pour ce qui

concerne ces catégories, dans la même situation qu'un Etat non contractant.

66. En ce qui concerne les «transferts» de données dont il est question au paragraphe 1, l'article 12 ne vise en effet que l'exportation de données et non pas leur importation qui de toute façon ne présenterait pas de problème puisque les données importées seraient assujetties au régime de protection des données de l'Etat importateur. Quelques problèmes pourraient par contre se poser en cas de réimportation de données traitées à l'étranger en violation de certaines dispositions du droit du pays d'origine partie à la Convention. Toutefois, il est évident dans ce cas qu'il appartient au pays d'origine de prendre avant l'exportation les mesures nécessaires aux termes de l'article 12.

67. Les paragraphes 2 et 3 s'appliquent aux mesures que les Etats peuvent prendre afin d'assurer que les flux transfrontières de données n'aient pas pour conséquence un affaiblissement de la protection des personnes se trouvant sur leur territoire ou à l'étranger par rapport aux traitements de données qui ont eu lieu partiellement ou entièrement sur leur territoire.

La règle principale (paragraphe 2) est qu'entre des Etats contractants il ne sera pas permis d'ériger des obstacles aux flux transfrontières de données, que ce soit sous forme d'interdictions ou d'autorisations spéciales. La raison fondamentale de cette règle est que, tous les Etats contractants ayant souscrit au «noyau dur» des dispositions en matière de protection des données énoncé au chapitre II, ils offrent un certain niveau minimal de protection.

Cette règle ne veut pas dire qu'un Etat contractant ne peut pas prendre d'autres mesures pour s'informer de la circulation de données entre son territoire et celui d'un autre Etat contractant, par exemple au moyen de déclarations obligatoires par les maîtres de fichiers.

L'expression «aux seules fins de la protection de la vie privée» apporte une clarification importante dans ce sens qu'un Etat contractant ne peut pas invoquer la Convention pour justifier une restriction à des flux transfrontières de données pour des raisons qui n'ont rien à voir avec la protection de la vie privée (par exemple des barrières déguisées au commerce).

Le paragraphe 2 de cet article n'affecte pas la faculté d'une Partie d'inclure dans sa législation interne en matière de protection des données des dispositions qui, dans des cas particuliers, n'autorisent pas certains transferts de données à caractère personnel, sans qu'il soit fait de distinction entre les transferts effectués à l'intérieur de son territoire ou à travers les frontières.

68. Il peut arriver dans certains cas que des transferts soient effectués à partir d'un fichier automatisé dans une Partie simultanément vers plusieurs pays étrangers dont certains sont parties à la Convention tandis que d'autres sont des Etats non contractants. Dans de tels cas, une Partie d'origine, qui a une procédure d'autorisation d'exportation, ne peut pas éviter que cette procédure soit appliquée également aux données destinées à une autre Partie, mais dans ce cas elle devra procéder de façon à assurer que l'autorisation soit donnée de plein droit aux transferts de données vers cette dernière Partie.

69. Les catégories de données ou de fichiers mentionnées au paragraphe 3.a peuvent être celles auxquelles allusion est faite à l'article 6, aussi bien que d'autres catégories. En ce qui concerne les données mentionnées à l'article 6 (par exemple origine raciale, opinions politiques), une Partie peut faire une dérogation aux termes de l'article 12, paragraphe 3.a, lorsque les mesures spécifiques de protection de ces données sont sensiblement différentes des dispositions du droit des autres Parties régissant ces données, et particulièrement lorsque ces mesures offrent, en conformité avec l'article 11, un niveau de protection allant au-delà des règles minimales énoncées au chapitre II. Une deuxième justification d'une dérogation peut se présenter lorsque des catégories de données ou de fichiers qui ne sont pas mentionnées expressément à l'article 6 sont assujetties à des garanties spéciales. Toutefois, il est clair qu'une dérogation au paragraphe 2 ne sera pas permise lorsque la Partie destinataire offre une protection équivalente. Ceci veut dire, entre autres, qu'un Etat contractant qui assujettit les flux transfrontières de données à une autorisation spéciale, ne peut pas refuser pour des raisons de protection de la vie privée, d'accorder une telle autorisation si le pays receveur octroie une protection équivalente.

70. La lettre *b* de ce paragraphe concerne les transferts de données vers un Etat non contractant à travers un Etat contractant. Le libellé de cet alinéa indique qu'une telle dérogation ne peut être invoquée que s'il est établi que les données transférées se trouvent dans un Etat contractant uniquement en transit. Elle ne doit pas être invoquée sur la base d'une seule présomption ou expectative, selon laquelle les données transférées à un autre Etat contractant pourraient éventuellement être réexportées vers un Etat non contractant. De même, un Etat qui aurait un système d'autorisation n'invoquera pas nécessairement la dérogation *b* dans le cas de tout trafic de données vers des Etats non contractants. Il peut décider de renoncer à de telles autorisations par exemple en raison du régime satisfaisant de protection des données appliqué par l'Etat non contractant en question.

Chapitre IV – Entraide

Article 13 – Coopération entre les Parties

71. Les dispositions principales de ce chapitre ont été inspirées par celles de deux récentes Conventions ayant trait à l'entraide en matière administrative: la Convention européenne sur la notification à l'étranger des documents en matière administrative du 24 novembre 1977 et la Convention européenne sur l'obtention à l'étranger d'informations et de preuves en matière administrative du 15 mars 1978. Pour ce qui est des Etats parties à ces Conventions, la conclusion d'un accord spécial dans le domaine de la protection des données est conforme à une disposition existant dans ces Conventions selon laquelle le cadre général de coopération créé peut être complété par d'autres accords dans des domaines spécifiques.

72. Parmi les raisons de préférer en l'occurrence un accord distinct, il y a lieu de rappeler que l'on s'attend à ce que la présente Convention attire un plus grand nombre d'Etats non-membres que les deux Conventions précitées. En outre, compte tenu de la nature spéciale de la protection des données, plusieurs Etats pourraient, en pratique, préconiser de confier l'assistance mutuelle en matière de protection des données à des instances spécialisées dans ce domaine. Du reste, dans la plupart des pays où la

protection des données est assurée par voie de législation, il existe une instance spécialement chargée de cette tâche et il n'est pas à exclure que cette instance soit désignée dans plusieurs Etats comme autorité de liaison au sens du *paragraphe 2.a*.

73. Il est à noter que si la Convention impose à chaque Partie la désignation d'une autorité, elle n'exige pas pour autant celle d'une autorité spécialement chargée de la protection des données. Une Partie pourrait désigner une autorité aux seules fins de la Convention.

74. Aux termes de l'article 13, les autorités désignées se prêteront mutuellement une assistance générale pour les contrôles à priori (par exemple en vue de certifier que les terminaux situés dans un pays A et reliés à un centre informatique situé dans un pays B sont bien conformes aux règles de sécurité des données) et une assistance spécifique pour les contrôles à posteriori (par exemple en vue de vérifier l'activité d'un centre de traitement particulier). Les informations échangées pourront être de caractère juridique ou factuelles.

75. En ce qui concerne les échanges d'informations juridiques entre Etats conformément au *paragraphe 3.a*, il a été suggéré que ces échanges pourraient être organisés non seulement bilatéralement entre Etats concernés mais aussi multilatéralement par l'intermédiaire du Secrétariat du Conseil de l'Europe. Une proposition dans ce sens a été élaborée séparément dans la Recommandation n° R (80) 13 relative à l'échange d'informations juridiques en matière de protection des données, qui a été adoptée par le Comité des Ministres le 18 septembre 1980.

76. Quant aux informations de fait, le *paragraphe 3.b* précise que les Etats ne se communiqueront pas les informations contenues dans les fichiers. Cette disposition vise de toute évidence à sauvegarder la protection de la vie privée des personnes concernées.

Article 14 – Assistance aux personnes concernées à l'étranger

77. Le *paragraphe 1* stipule que les personnes concernées ayant leur résidence à l'étranger, dans un Etat contractant ou un Etat tiers, seront habilitées à exercer leur droit de connaître, et le cas échéant de rectifier, les informations enregistrées sur elles dans un fichier. Ceci est une conséquence pratique de l'article 1 qui assure une protection à «tout individu quelles que soient sa nationalité ou sa résidence».

78. Aux termes du *paragraphe 2*, lorsque la personne concernée réside dans un autre Etat contractant, elle aura la faculté d'exercer ses droits directement dans le pays où les informations la concernant sont traitées, ou indirectement par l'intermédiaire de l'autorité désignée par son pays de résidence.

En outre, il va sans dire que les personnes concernées ayant leur résidence à l'étranger ont toujours la faculté de faire valoir leurs droits avec l'assistance des agents diplomatiques ou des fonctionnaires consulaires de leur propre pays.

Le *paragraphe 3* stipule, afin d'accélérer la procédure et éviter les abus, que les demandes doivent être aussi précises que possible.

Article 15 – Garanties concernant l'assistance

79. Cet article prévoit que les autorités de protection des données seront liées par la même obligation d'observer la discrétion et la confidentialité à l'égard des autorités étrangères de protection des données et des personnes résidant à l'étranger, que celles qu'elles observent dans leur propre pays.

Cette disposition revêt une importance fondamentale pour la confiance réciproque sur laquelle l'assistance mutuelle repose.

Article 16 – Refus de demandes d'assistance

80. Cet article stipule que les Parties sont tenues de donner suite aux demandes d'assistance. Les motifs de refus sont limitativement énumérés. Ils correspondent d'une manière générale à ceux prévus par d'autres conventions internationales d'entraide.

L'on peut opposer un refus si la demande est incompatible avec les compétences de l'autorité ou avec les termes de la Convention et notamment avec son article 3 visant le champ d'application compte tenu des extensions et exclusions que chaque Partie y aura éventuellement apportées, ou si elle est en contradiction avec des intérêts prédominants de l'Etat requis ou de la personne concernée.

81. L'expression «exécution» utilisée à la lettre c devrait être entendue dans un sens large couvrant non seulement la réponse à la demande, mais aussi l'activité qui la précède. Par exemple, une autorité requise pourrait refuser d'agir non seulement si la transmission à l'autorité requérante de l'information demandée pouvait porter préjudice aux droits fondamentaux de l'individu, mais également si le fait même de rechercher l'information constitue un risque d'atteinte à ces droits.

Article 17 – Frais et procédures de l'assistance

82. Les dispositions de cet article sont analogues à celles d'autres conventions internationales d'entraide.

83. La notion d'«experts» dans le sens du *paragraphe 1* comprend notamment les informaticiens dont on demande l'intervention pour effectuer des tests sur l'ordinateur ou contrôler la sécurité d'un fichier automatisé.

84. Afin de ne pas alourdir la Convention par une multitude de détails d'exécution, le *paragraphe 3* de cet article prévoit que la procédure, les formes et la langue à utiliser peuvent être convenues entre les Etats concernés. Le libellé de ce paragraphe n'exige pas qu'il s'agisse de procédures formelles, mais admet également des arrangements administratifs portant même sur des cas concrets. Il est souhaitable en outre que les Etats délèguent aux autorités désignées le pouvoir de conclure de tels arrangements. Les formes de l'assistance pourront également varier suivant les cas. Il est évident par exemple, que la transmission d'une demande d'accès à des informations médicales sensibles exigera des formalités différentes de celles suivies pour des enquêtes de routine sur des inscriptions figurant dans un registre de population.

Chapitre V – Comité consultatif

85. Le but des articles 18, 19 et 20 est de faciliter l'application de la Convention et, si nécessaire, de perfectionner celle-ci.

86. Puisque la Convention contient un nouveau genre de droit, créé pour résoudre les problèmes nouveaux posés par le traitement automatisé des données, on peut s'attendre à ce que des questions se posent tant en ce qui concerne l'application pratique de la Convention (article 19, lettre *a*) que pour ce qui est de son interprétation (même article, lettre *d*);

Un Comité consultatif composé de représentants de toutes les Parties s'efforcera de formuler des propositions ou de donner des avis à ces Parties en vue de la solution de ces problèmes.

Lorsque cela s'avérera nécessaire, le Comité proposera lui-même des amendements à la Convention ou examinera les propositions formulées par une Partie ou par le Comité des Ministres conformément à l'article 21.

87. La nature du Comité et les procédures suivies sont analogues à celles créées aux termes d'autres conventions conclues dans le cadre du Conseil de l'Europe.

Il n'a pas été jugé souhaitable que le Comité prenne la forme d'une autorité internationale pour la protection des données. De même, il n'a pas été estimé opportun de lui confier le règlement formel de différends pouvant surgir de, l'application de la Convention. Il est cependant évident que le Comité peut contribuer à résoudre les difficultés qui surgissent entre Parties.

Chapitre VI – Amendements

Article 21 – Amendements

88. Le Comité des Ministres, au sein duquel le texte original de cette Convention a été adopté, est aussi compétent pour l'approbation de tout amendement.

Conformément au *paragraphe 1*, l'initiative des amendements peut être prise par le Comité des Ministres lui-même, par le Comité consultatif et par une Partie (qu'il s'agisse d'un Etat membre du Conseil de l'Europe ou non).

Toute proposition d'amendement ne provenant pas du Comité consultatif doit lui être soumise pour avis aux termes du *paragraphe 3*

Chapitre VII – Clauses finales

Article 22 – Entrée en vigueur

89. Etant donné qu'il a été considéré comme essentiel pour l'efficacité de la Convention qu'elle ait un large champ d'application géographique, le *paragraphe 2* fixe à cinq le nombre de ratifications d'Etats membres du Conseil de l'Europe nécessaires pour son entrée en vigueur.

Article 23 – Adhésion d'Etats non-membres

90. La Convention a été conçue comme «ouverte» avec un large champ d'application géographique (voir paragraphes 14 et 15). La Convention ayant été élaborée en étroite collaboration avec l'OCDE et les Etats membres non européens de cette Organisation, ce sont notamment ces pays auxquels on a pensé lors de la rédaction de cet article.

Article 24 – Clause territoriale

91. L'application de la Convention à des territoires lointains placés sous la juridiction des Parties ou au nom desquels une Partie peut s'engager revêt une importance pratique, importance tenant à l'utilisation de pays éloignés pour les opérations de traitement de données tant en raison du coût et de la main-d'œuvre que pour l'utilisation de la capacité alternée de traitement pendant la nuit et le jour.

Article 25 – Réserves

92. Les règles contenues dans cette Convention constituent les éléments les plus fondamentaux et essentiels pour une protection efficace des données. Pour cette raison la Convention n'admet pas de réserves à ses dispositions qui gardent, toutefois, une souplesse raisonnable compte tenu des possibilités offertes par l'article 3 (champ d'application) et des dérogations admises par certains autres articles.

Article 26 – Dénonciation

Article 27 – Notification

93. Ces dispositions sont conformes aux clauses finales habituelles contenues dans les conventions européennes.