COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 21 juin 2011 T-PD-BUR(2011) 10 fr

Rapport sur la consultation relative à la modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Auteurs :

Cécile de Terwangne professeur à la Faculté de Droit, directrice de recherche au CRIDS, Université de Namur (FUNDP) - Belgique

Jean-Philippe Moiny, chercheur au CRIDS, doctorant FNRS, Université de Namur (FUNDP) - Belgique

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

Les vues exprimées dans ce rapport relèvent de la responsabilité des auteurs et ne reflètent pas nécessairement la position officielle du Conseil de l'Europe.

TABLE DES MATIERES

Introduction

1. La consultation publique lancée par le Conseil de l'Europe pour recueillir les réactions de toutes les parties concernées sur la perspective de modernisation de la Convention 108 a remporté un franc succès. De nombreuses contributions sont parvenues au Secrétariat du Conseil de l'Europe. Ces contributions sont le plus souvent approfondies et étayées par des arguments ou analyses bénéficiant de l'expertise ou de l'expérience de terrain des contributeurs. Par ailleurs, certains intervenants se sont groupés pour présenter une réaction commune au questionnaire et d'autres, en tant que fédérations ou groupements, se sont exprimés au nom de tous leurs membres.
2. Tous les horizons sectoriels sont représentés parmi les répondants : des acteurs issus tant du secteur public (autorités gouvernementales, autorités de protection des données,…) que du secteur privé (monde bancaire, des assurances, du commerce électronique, du marketing, de la diffusion audio-visuelle, de la recherche socio-économique,…), ainsi que du monde universitaire et des associations intéressées.
3. Une représentation géographique variée s'observe aussi. Ainsi, les réponses proviennent des différentes zones de l'Europe. Les pays de l'Union européenne sont concernés mais également des pays hors de l'UE, comme l'Albanie ou l'Ukraine. Il est intéressant de pouvoir comparer les réponses issues de pays couverts par la directive européenne relative à la protection des données (zone UE) avec celles venant d'autres pays qui ne le sont pas. Par ailleurs, des contributions sont parvenues d'Amérique du Nord (Etats-Unis et Canada), de l'Afrique (Sénégal, Ile Maurice), de l'Australie. L'organisation internationale de la Francophonie a également émis un commentaire.

Considérations générales

4. Parfois les réponses obtenues signalent une orientation à suivre mais n'apportent pas d'indication sur le moyen de concrétiser cette orientation. Parfois, au contraire, les commentateurs présentent des arguments et des pistes pour aller dans telle ou telle direction.
5. Dans une série de cas, les contributeurs annoncent qu'au vu de la difficulté de la question, il conviendrait de réaliser une étude approfondie. C'est le cas par exemple pour l'exclusion du champ d'application des traitements de données à des fins personnelles et domestiques ou pour la question du droit applicable. Dans d'autres cas, c'est à une analyse d'impact ou à une étude d'efficacité des mesures législatives envisagées qu'invitent les contributeurs (notamment concernant l'introduction de la possibilité des recours collectifs et de systèmes d'*alternative dispute resolution*, ou concernant l'instauration d'un devoir de signaler les violations de données – *data breaches*).
6. De très nombreux contributeurs ont plaidé pour que le travail de modernisation de la Convention soit effectué en ayant le souci d'établir la plus grande cohérence avec les règles de protection édictées par l'Union européenne (principalement la directive 95/46). Dans bien des cas les réponses sont donc orientées par cette préoccupation d'aligner le texte de la Convention sur celui de la directive européenne. Il est demandé de suivre les travaux de modernisation de cette directive actuellement en cours pour veiller à ne pas faire naître des divergences entre les textes. Il est intéressant de souligner que cette préoccupation n'est pas formulée par les seuls acteurs issus de pays de l'Union européenne. Elle est partagée par des acteurs situés hors de l'UE.

Objet et champ d'application de la Convention, Définitions

1. Rédigée selon une approche « technologiquement neutre », la Convention 108 est un instrument général et simple : peut-on conserver cette approche ou doit-on au contraire élaborer un texte plus détaillé ?

7. L'ensemble des répondants s'est prononcé en faveur du maintien d'un texte simple, énonçant des principes généraux.
8. Cette approche est à leurs yeux la seule qui puisse garantir la viabilité à long terme de la Convention. Les trente années écoulées avec une Convention consacrant des principes généraux ont démontré que ce modèle passait positivement l'épreuve du temps.
9. Dans la même perspective de durée, tous soulignent également la nécessité de veiller au caractère technologiquement neutre de la Convention. La formulation des principes ne doit pas être focalisée sur l'existence d'une technologie. Cela présenterait le double risque de désuétude des principes dès que la technologie sera dépassée ou abandonnée et d'inadaptabilité de ces principes aux nouvelles technologies qui ne manqueront pas d'émerger.
10. Cela étant dit, les répondants indiquent que, tout en ne transformant pas le texte de la Convention en un texte trop détaillé, il s'impose tout de même d'apporter certains compléments au texte existant.
11. Plusieurs contributeurs attirent l'attention sur le fait que si la Convention doit désormais avoir une vocation universelle, il faut être conscient qu'un texte trop détaillé fera assurément peur aux Etats qui envisageraient leur éventuelle adhésion à la Convention.
12. Le modèle existant devrait donc être poursuivi, selon certains : conserver un caractère général et simple au texte de la Convention et détailler les principes généraux dans des textes spécifiques (recommandations du Comité des ministres).

2. La Convention 108 devrait-elle définir le droit à la protection des données et le droit au respect de la vie privée ?

13. Certaines des personnes ayant répondu à cette question estiment qu'intégrer des définitions du droit à la protection des données et du droit au respect de la vie privée aiderait à clarifier la portée du texte et aiderait le public à percevoir le champ de la matière. Cela mettrait notamment en lumière, aux yeux de l'APEP – Association Professionnelle Espagnole de la Vie privée, que la vie privée et la protection des données sont deux droits différents, les données à caractère personnel pouvant d'ailleurs être privées ou non.
14. D'autres estiment que la notion de vie privée apparaissant dans plusieurs instruments juridiques internationaux, il ne serait pas opportun de la définir dans la Convention 108. Il appartient à la Cour européenne des droits de l'homme, notamment, de définir la portée de cette notion reprise à l'article 8 CEDH. Pour la CNIL, par exemple, il ne faut pas définir ces notions pour leur permettre d'être interprétées de façon évolutive. Le State Data Protection Inspectorate de Lituanie relève que les instruments juridiques internationaux qui protègent la vie privée ne contiennent aucune définition de celle-ci. La même approche pourrait être suivie en ce qui concerne le droit à la protection des données.

15. Signalons au passage que les contributions laissent entrevoir une perception non homogène de ce qu'est la vie privée/privacy. Dans plusieurs contributions, c'est l'évocation du sens classique (intimité, confidentialité) qui est mentionnée et non le sens plus évolué d'autonomie et de maîtrise informationnelle qui a été mis au jour par la Cour européenne des droits de l'homme. La European Banking Association qui estime que la Convention 108 devrait contenir les définitions en question précise d'ailleurs que cela doit être particulièrement fait dans la mesure où la Convention doit servir de base à des pays situés hors de la zone de l'Espace Economique Européen et qui ne disposent pas de définitions spécifiques dans leur propre législation et n'ont aucune connaissance de l'évolution des notions de « vie privée/privacy » et de « protection des données » dans la jurisprudence et la doctrine en lien avec les définitions européennes existantes.
16. Par contre, pour ce qui est de la notion de droit à la protection des données, ces contributeurs et d'autres perçoivent l'intérêt d'une définition tout en incitant à l'harmoniser avec celle se trouvant dans la Charte des droits fondamentaux de l'Union européenne. Privacy International souligne en ce sens qu'il vaudrait la peine de songer à définir le droit à la protection des données étant donné que de nombreuses constitutions dans le monde ont commencé à reconnaître que la protection des données est effectivement un droit.
17. Certains répondants trouvent qu'il ne se justifie pas de définir les notions après 30 ans d'application du texte. L'ancienneté du texte fait réagir dans un sens opposé la Direcçao Geral da Politica de Justiça du Portugal qui estime qu'en tant que le plus ancien instrument juridique de droit international public en la matière, la Convention 108 qui prétend régler le droit à la protection des données ne peut se montrer incapable de définir elle-même ce droit.
18. Ne se prononçant pas sur l'opportunité d'introduire de telles définitions, l'European Newspaper Publishers Association demande que si l'on opte pour une définition, on veille à ne pas induire que ces droits prévaudraient sur ceux de la liberté d'expression et d'information. Il faut également veiller à ne pas introduire d'insécurité juridique.

3. La Convention 108 protège les individus contre toute atteinte portée à leur vie privée par des autorités privées et publiques, y compris la police et la justice. Cette approche globale doit-elle être conservée ?

19. Il y a unanimité pour considérer qu'il faut conserver une approche couvrant tant le secteur privé que l'ensemble du secteur public, incluant donc la police et la justice. Etant donné les facilités pratiques et le potentiel des outils techniques existants (sans compter ceux qui apparaîtront à l'avenir), il est considéré comme « absolument vital », pour reprendre les termes de nombre de contributeurs, d'imposer aux acteurs de la police et de la justice le respect de principes de protection des données.
20. Bien sûr tout le monde s'accorde sur la nécessité d'aménagement de ces principes pour prendre en compte les nécessités liées au travail de ces acteurs. L'important est de ne pas faire sortir purement et simplement la justice et la police du champ de la protection. Ce qui est envisagé c'est généralement un régime d'exceptions partielles au bénéfice de ces acteurs.
21. TechAmerica Europe propose que l'on réfléchisse à des situations dans lesquelles des règles différentes partielles existeraient pour les autorités publiques et pour les entités privées, tout en gardant les mêmes principes de base et exigences de transparence. Ils invitent à prendre en considération l'impact que les modifications de la Convention pourront

avoir sur le travail de la police et de la justice pour vérifier que ces nouvelles mesures ou nouveaux concepts ne suscitent pas des difficultés particulières pour ce secteur.

22. Un autre contributeur américain demande que l'on soit attentif à ce que tout changement que l'on apporterait à la Convention continue de permettre un degré de flexibilité des échanges de données « policières » entre Etats-Unis et Europe et autorise le partage de données à des fins de sécurité publique et de poursuite des infractions.

23. Les contributeurs canadiens ont souligné que l'expérience de deux régimes séparés pour les secteurs public et privé qu'ils connaissent au niveau fédéral chez eux a fait l'objet de critiques émanant de la société civile et du *Federal Privacy Commissioner*.

4. La Convention 108 n'exclut pas de son champ d'application les données traitées par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. Doit-on maintenir cette approche, ou au contraire introduire une exception dans ce cas précis (dans le contexte spécifique du Web 2.0.) ?

24. De façon générale les répondants sont favorables à l'introduction d'une exclusion du champ d'application de la Convention des traitements de données effectuées à des fins personnelles ou domestiques.

25. De nombreux répondants soulignent que cela doit se faire dans le souci d'aligner le modèle de protection de la Convention sur celui de la directive 95/46.

26. Toutefois plusieurs contributeurs sont d'avis qu'il sera particulièrement difficile de définir ce qui serait précisément visé par une telle exclusion.

27. L'AEDH, favorable à cette exclusion, propose de la soumettre à la condition qu'il n'y ait pas transmission de données à des tiers et d'accompagner cette exclusion d'une obligation pour les services qui serviraient de support à de telles activités personnelles (messagerie électronique, carnet d'adresses, agenda, service d'archivage,…) d'informer leurs clients sur leurs obligations et de leur offrir des fonctions de confidentialité.

28. La CNIL invite à reprendre le modèle de l'Union européenne et dire qu'il relève du pouvoir d'interprétation des autorités de contrôle nationales de préciser ce qui relève ou non de l'exception.

29. Le CIPPIC (Canada) relève que cette question a été mentionnée comme un des défis à venir en matière de protection des données. Il convient en tout cas d'effectuer une prudente mise en balance avec le droit à la liberté d'expression lorsque l'on veut régler cette question du sort des activités privées des individus. C'est précisément à l'occasion de leur réflexion sur la liberté d'expression confrontée à la protection des données que le Centre for Socio-Legal Studies a développé son point de vue sur cette hypothèse d'exclusion. Réalisant que beaucoup de situations dans lesquelles des données personnelles sont traitées de la façon la plus intrusive et la plus injustifiable sont de plus en plus souvent le fait de personnes privées mues par des raisons non commerciales, ce Centre ne souhaite pas voir ces activités exclues de toute règle de protection. A ses yeux une meilleure solution consisterait d'abord à s'assurer que de telles activités individuelles puissent bénéficier pleinement d'une disposition nouvelle plus large sur la liberté d'expression et ensuite à imposer aux individus seulement certaines des obligations des responsables de traitement, déterminées de manière claire et proportionnée.

30. La European Privacy Association, rejointe sur ce point par l'APEP (Association Professionnelle Espagnole de la Vie privée) et par le State Data Protection Inspectorate de

Lituanie, soulève que les activités des individus peuvent aujourd'hui porter facilement atteinte à d'autres et qu'on ne peut donc exclure totalement leurs activités des règles de protection des données. Mais par contre, on ne peut soumettre des activités purement personnelles à des obligations et charges disproportionnées, notamment en matière de sécurité (article 7) et concernant les flux transfrontières (article 12). L'APEP insiste sur le fait que la régulation doit pouvoir sanctionner les usages abusifs de données à caractère personnel commis par des particuliers. Cette association estimerait pour sa part disproportionné que l'on impose aux utilisateurs particuliers des obligations telles que celle de déclarer le traitement de données, de fournir des informations dans la ligne des articles 10 et 11 de la directive 95/46, d'adopter des mesures de sécurité ou de veiller à ce que de telles mesures soient implémentées par la plateforme qu'ils utilisent.

31. La Commission à la protection des données du Sénégal suggère qu'au-delà de l'exclusion proposée qu'elle soutient, on élargisse cette exclusion en y ajoutant « les traitements dont les données ne sont pas destinées à une communication systématique à des tiers ou à la diffusion ».

5. La définition du traitement automatisé n'inclut pas la collecte des données : le fait que la collecte fasse l'objet d'une disposition spéciale est-il problématique ? Est-ce suffisant ? Doit-on ajouter d'autres opérations à la liste existante ?

32. Tous ceux qui se sont exprimés sont favorables à l'inclusion de la notion de collecte dans celle de traitement automatisé. C'est tout d'abord la volonté de garantir une cohérence avec les normes européennes, nationales et internationales qui motive cette position. Ensuite, c'est la conviction qu'il est utile que la collecte soit soumise à l'ensemble des principes régissant les traitements de données et non à une seule disposition particulière.

33. Le souci de cohérence entre les ordres juridiques explique aussi que de nombreux contributeurs comme le CEA Insurers of Europe ou l'AFME BBA (banking & financial services) réclament l'adoption de la notion de « traitement » (« *processing* ») telle que présentée dans la directive européenne. Pour le CEA, il serait utile que l'opération de « communication par transmission » (« *disclosure by transmission* »), opération fondamentale dans le traitement des données, soit expressément reprise dans la liste des opérations couvertes. Pour la CNIL, la notion de traitement devrait être la plus large possible, tant les opérations réalisées sur les données ont tendance à se multiplier et se diversifier.

34. L'AFME BBA de même que l'European Banking Federation relève qu'il faut s'assurer que la terminologie ne soit pas confinée à des concepts comme celui de « fichier » qui ont une connotation technologique datée qui pourrait compromettre à la fois la neutralité du texte et une large application de la Convention, étant donné que cette notion n'a plus de pertinence dans la réalité d'Internet et du *cloud computing*.

35. Enfin, la Direcçao Geral da Politica de Justiça du Portugal invite à réfléchir à l'élargissement du champ d'application de la Convention afin d'y inclure les traitements non automatisés. Conscient que ces traitements sont minoritaires aujourd'hui, cet organe estime toutefois qu'ils n'ont pas entièrement disparu et que la prudence indique de les intégrer dans le champ de la protection.

La définition du maître de fichier devrait être revue : plusieurs critères doivent-ils être répertoriés, ces critères doivent-ils se cumuler, peut-il y avoir plusieurs maîtres de fichier pour un seul fichier?

36. Pour certains répondants, la Convention dans sa version actuelle ne doit pas être amendée sur ce point. Les définitions actuelles suffisent à rendre responsables les personnes impliquées dans le traitement des données.
37. Pour d'autres, la définition du « responsable du traitement/data controller » issue de la directive 95/46 devrait se substituer à celle de maître de fichier.
38. Le Commissaire à la protection des données de l'Ile Maurice propose de renouveler la définition par la définition suivante : « le maître du fichier est toute personne physique ou morale, publique ou privée, qui décide de toute activité, automatisée ou non, entreprise sur des données personnelles. ». L'APEP - Association Professionnelle Espagnole de la Vie privée propose pour sa part de revoir la définition de manière à inclure « celui/ceux qui de facto a/ont le droit de décider du but et des moyens du traitement de données à caractère personnel, soit par effet de la loi, soit en vertu d'accord contractuel avec la personne concernée ou avec un tiers. ». Par souci de sécurité juridique, cet organisme trouve important que l'on limite les responsables de traitement aux personnes ayant la personnalité juridique.
39. Plusieurs signalent qu'il serait opportun de prévoir l'hypothèse où il y a plusieurs responsables pour un même traitement de données. L'AEDH donne l'exemple de la décision de mise en œuvre d'un fichier prise par un ensemble de responsables à des fins collectives, comme l'élaboration d'un fichier commun à une profession relatif à des clients défaillants. L'APEP fait la distinction entre les contrôleurs joints (en cas de traitement des mêmes données dans le même but) et plusieurs contrôleurs (en cas de traitement des mêmes données mais dans des buts différents).
40. La European Privacy Association attire l'attention sur le fait que de plus en plus les technologies développées (comme celle du *cloud*) conduisent à ce que des données soient traitées de manière automatisée par de multiples intervenants. Pour cette association, il est important non de définir le nom et le rôle de ces intervenants mais plutôt leurs activités de traitement, les charges et obligations en lien avec ces activités et les responsabilités liées. Le Information Commissioner for the United Kingdom's (ICUK) abonde dans le même sens lorsqu'il dit que, plutôt que lister des critères concernant ce qui constitue un « *controller* », il préfèrerait que l'on fournisse une meilleure description des activités qu'un maître de fichier peut entreprendre.
41. Pour EFAMRO ESOMAR (secteur de la recherche), il faudrait introduire une définition clarifiée du "responsable du traitement" qui placerait les responsabilités sur ceux qui décident comment les données vont être traitées par opposition à ceux qui contrôlent un système informatique ou un fichier particuliers. Cela ferait reposer sur un seul responsable du traitement la responsabilité d'évaluer la nécessité de traiter des données et la sécurité des systèmes disponibles avant d'opter pour le traitement de données avec de tels systèmes. Cela assurerait en outre un point unique de responsabilité et d' « accountability » pour les citoyens.
42. La German Insurance Association accueillerait favorablement une révision de la notion de maître du fichier car cela donnerait l'opportunité d'introduire des changements dans le traitement des données dans le monde des affaires. C'est principalement la centralisation des tâches de service au sein des groupes et le recours à l'outsourcing de tâches à des services compétents qui sont concernés. Pouvoir présenter l'entité qui transfère les

données et celle qui les reçoit de manière jointe comme un responsable unique du traitement faciliterait les transferts de données et simplifierait la vie des groupes.

43. Cette position va dans le même sens qu'une remarque du consortium Computer Law and Security Review, International Association of IT Lawyers and the Institute for Law and the Web (University of Southampton) : ils relèvent que dans un environnement en réseau, la notion de responsable du traitement n'a plus la pertinence d'antan, étant donné l'usage croissant de systèmes de partage et de mise en relation de données. Dans de tels environnements, il serait préférable de nommer une seule entité comme assumant la responsabilité générale (comme dans les systèmes de *binding corporate rules* de l'UE). Il conviendrait d'imposer l'obligation aux responsables de traitement individuels d'informer les personnes concernées des partages et mises en relation de données auxquels ils participent ainsi que des coordonnées de l'entité de coordination.
44. Enfin, Mydex Community Interest Company signale – et dit que sa vision est partagée par de nombreux autres, incluant le World Economic Forum – qu'à l'avenir les architectures techniques des prochaines générations placeront les individus au centre de leur propre éco-système de données à caractère personnel, assumant donc eux-mêmes le rôle de responsable de traitement. La législation devra refléter ce nouveau modus operandi et permettre ce « data empowerment by design ».

6. De nouvelles définitions sont peut-être nécessaires, comme celle du sous-traitement ou celle du fabricant des équipements techniques.

45. Les contributeurs saluent l'intention d'introduire de nouvelles définitions si cela se fait dans un souci de cohérence avec celles développées au sein de l'UE. Cela permettrait d'augmenter la sécurité juridique, d'améliorer la protection des personnes concernées et d'éviter de créer la confusion pour les responsables de traitement.
46. Plusieurs signalent avec bon sens qu'il est clair qu'il n'y a de sens à insérer la définition d'acteurs supplémentaires que si un régime juridique particulier fixant des obligations est attaché à ces nouveaux acteurs.
47. Plusieurs estiment indispensable l'ajout de la définition du sous-traitant. Le Garante per la protezione dei dati personali italien relève en outre que le besoin d'introduire une telle définition s'est déjà fait sentir dans plusieurs résolutions du Conseil de l'Europe (la Recommandation 2002(9) sur la protection des données dans le secteur des assurances et la Recommandation 2010(13) sur le profilage).
48. Pour Privacy International, par contre, le concept de « sous-traitant » n'est plus utile étant donné que des sous-traitants, dans la réalité, doivent assumer de si nombreux devoirs de sécurité et de respect de la vie privée que leur rôle devient très difficile à distinguer. Il est problématique de demander à des responsables de traitement d'être responsables des mesures de vie privée et de sécurité alors que dans les faits ils sont entièrement dépendants des conditions contractuelles établies par des fournisseurs de service (du *cloud* notamment) non soumis à la régulation.
49. La German Insurance Association demande que cette définition soit flexible et autorise, selon les circonstances, que la maison mère puisse aussi être mandatée par une société du groupe comme sous-traitant, mais que, dans ce cas, il y ait des limites pour reconnaître le droit d'émettre des instructions selon le droit existant.

50. L'AEDH propose qu'une nuance soit introduite pour les fournisseurs de service traitant des données pour le compte du responsable du traitement mais jouissant d'une claire autonomie pour réaliser le service, de sorte qu'ils portent une double casquette de responsable du traitement et de sous-traitant. Dans cette hypothèse, on pourrait introduire la notion de "person entrusted" "personne chargée" du traitement, à qui le traitement est confié: lorsque le sous-contractant agit strictement au nom et sur les instructions du responsable du traitement et n'est pas responsable comme un responsable de traitement, la personne chargée du traitement pourrait être considérée comme supportant une part de la responsabilité, conjointement ou totalement.

51. Pour le ICUK, la simple distinction entre un responsable et un sous-traitant ne reflète plus les relations compliquées qui existent entre les organisations qui traitent des données personnelles. Le modèle des définitions de la directive 95/46 correspond à un sous-traitant passif n'agissant que sur instructions du responsable, alors que dans la réalité celui qui apparaît comme un sous-traitant peut exercer une influence considérable sur la manière dont le traitement prend place et peut, sur bien des aspects, agir comme un responsable de traitement. Pour la CNIL, cette situation où effectivement, de façon croissante, le traitement effectif et quotidien des données se situe dans les mains du sous-traitant et non dans celles du responsable de traitement, conduit à imposer de définir cette catégorie d'acteur. Pour cette autorité, une cohérence avec la définition de la directive précisant qu'il s'agit de l'organisme « agissant pour le compte » du responsable de traitement est nécessaire. Cet organisme plaide encore pour que le régime de responsabilité du sous-traitant soit davantage harmonisé et encadré au niveau européen.

52. Quant à l'ajout d'une définition du "fabricant d'équipements techniques", certains comme l'European Banking Association estiment que c'est une bonne approche de l'envisager, alors que pour l'AEDH, c'est carrément indispensable, que les équipements en question soient matériels ou logiciels. Le Cyberspace Law and Policy Centre (Australie) de même que le Commissioner for Personal Data Protection de Chypre et le consortium CLSR-IAITL-ILAWS notent que cela s'avérera nécessaire si l'on introduit des dispositions concernant le *Privacy by Design* – ce que l'autorité chypriote ne souhaite pas à l'inverse des autres.

53. Le Garante italien a une approche plus nuancée : il estime qu'il serait indubitablement utile d'édicter les garanties qui devraient être offertes par toute entité additionnelle qui prendrait part au traitement d'une façon ou d'une autre (tel que le fabricant d'équipement technique), tout en faisant peser sur le responsable du traitement l'obligation juridique de vérifier le respect de ces garanties.

54. Pour Privacy International, par contre, il ne serait pas sage de définir les fabricants d'équipement hors d'un risque spécifique pour la vie privée et d'un contexte de sécurité. La Direcçao Geral da Politica de Justiça du Portugal est elle aussi opposée à l'inclusion de cette notion, n'en voyant pas l'utilité.

Principes de protection

7. De nouveaux principes pourraient être ajoutés à la Convention, comme le principe de proportionnalité qui devrait s'appliquer à l'ensemble des opérations réalisées sur les données. Ce principe est également lié au principe de minimalisation des données qui vise à limiter la collecte des données à caractère personnel au strict minimum, voire à y mettre un terme quand cela est possible.

55. Pour beaucoup, le principe de proportionnalité est déjà compris dans l'article 5 de la Convention. Ils réduisent donc ce principe à son application quant aux données qui doivent être pertinentes et non excessives.

56. D'autres répondants trouvent qu'il serait recommandable d'inclure les principes de proportionnalité et de minimisation ou limitation de la collecte des données dans les principes de protection, certains disant que ces principes doivent passer de la forme implicite à une formulation explicite. La formulation expresse de ces principes permettrait d'en définir précisément et mieux l'étendue. Notamment cela permettrait de stipuler que le principe de proportionnalité s'applique à toutes les opérations et pas seulement à la collecte (Cyprus Commissioner). Autrement dit, le principe de proportionnalité lié à la finalité de chaque opération du traitement (Garante) ou le critère du caractère non excessif de l'ensemble d'un projet de traitement de données particulier au regard des libertés et droits fondamentaux en cause doit être posé, cumulativement à la nécessité de minimiser les données traitées (AEDH). Dans le même sens l'AEDH dit que le principe de minimisation des données ne doit pas remplacer celui de proportionnalité car celle-ci doit dépasser les seules données.

57. Certains contributeurs appuient fortement l'insertion de ces principes qu'ils estiment très importants (CLPC, Australie ; APEP-Association Professionnelle Espagnole de la Vie privée ; Czech Office for personal data protection ; CLSR-IAITL-ILAWS ; Garante italien).

58. Morpho-Groupe Safran (technologies d'identification) qui voit dans le principe de proportionnalité un principe « qui vise à assurer un équilibre entre le traitement des données et la finalité poursuivie » se méfie de la démarche subjective qu'implique l'application de ce principe. Cette subjectivité débouche sur des divergences entre autorités de protection des données nationales dans l'acceptation ou non d'un produit ou dispositif industriel. Ils souhaitent en conséquence que si ce principe était consacré dans la Convention, il s'accompagne de dispositions de nature objective, telles qu'encourager le recours à des procédures de labellisation/certification reposant sur des critères précis que l'industriel devrait respecter pour développer ses produits.

59. Pour la GDD (association allemande pour la protection des données et la sécurité des données), il faudrait accorder certains avantages aux organisations qui recourent à des pseudonymes plutôt qu'à des données directement reliées à des personnes.

60. ARD et ZDF (radio et télévision) estiment qu'alors que l'utilisateur de médias traditionnels a toujours bénéficié d'un complet anonymat, cela n'est plus vrai pour les services proposés via Internet. En conséquence, ils soutiennent fermement le principe de limiter strictement la collecte de données au but poursuivi.

61. CEA Insurers of Europe demande que la minimisation des données soit présentée comme un objectif et non comme une obligation.

8. La question du consentement devrait-elle être envisagée en étroite liaison avec le principe de transparence et l'obligation d'informer, ou en tant que condition nécessaire à satisfaire un traitement loyal et licite avant toute autre action ?

62. Pour plusieurs contributeurs, il faut relativiser le rôle du consentement comme base légale pour le traitement de données. En tout cas il ne devrait pas servir comme seule base. Pour certains il ne devrait pas être présenté du tout comme condition pour satisfaire un traitement loyal et licite. Dans bien des cas les personnes qui consentent ne se rendent pas compte de ce à quoi elles ont consenti. Le consentement n'est ni une garantie de protection pour les personnes concernées, ni une solution praticable pour les responsables de traitement pour qui il peut représenter un fardeau disproportionné (dans le monde du marketing ou celui des assurances, par exemple).
63. Une grande peur règne quant à la qualité du consentement. Des problèmes de vraie liberté du consentement sont pointés, de même que par rapport à la forme que l'on donne de plus en plus au consentement.
64. Sur ce point, la GDD (association allemande pour la protection des données et la sécurité des données) estime que le modèle de la loi allemande en la matière offre une bonne protection aux consommateurs. Cette loi stipule que si le consentement est donné dans une forme différente que par écrit, le responsable du traitement doit donner une confirmation écrite de la substance du consentement à la personne concernée, à moins que le consentement ait été donné sous forme électronique, auquel cas le responsable doit conserver un enregistrement du consentement auquel la personne concernée doit pouvoir accéder et qu'elle peut révoquer à tout moment avec effet pour le futur.
65. Le CLPC (Australie) propose, quant à lui, le modèle de la loi canadienne régulant la protection de la vie privée dans le secteur privé (PPIPEDA). Une proposition d'amendement de cette législation est particulièrement intéressante : « le consentement d'un individu est seulement valide s'il est raisonnable de s'attendre à ce que l'individu comprenne la nature, le but et les conséquences de la collecte, de l'utilisation ou de la divulgation de l'information personnelle auxquelles il consent ». Pour le CLPC, si on introduit la notion de consentement, il faut que celui-ci soit expressément défini comme libre, informé et révocable, et non lié à d'autres consentements. Il faudrait également un principe général disant que lorsqu'un consentement véritable est une option réaliste, il devrait être le fondement privilégié d'un traitement légitime, ce qui serait cohérent avec le but global de transparence des traitements de données à caractère personnel.
66. La US Federal Trade Commission relève qu'éliminer le choix des personnes concernées pour les pratiques évidentes pour les consommateurs, permet de redonner sens aux choix à faire pour des pratiques plus problématiques (comme transférer leurs données à des tiers qui n'ont rien à voir avec la finalité du traitement des données).
67. De nombreux répondants ont insisté sur le fait que le consentement doit être lié à la transparence. Pour Privacy International c'est même la transparence qui prime le consentement, dans le sens où il faut privilégier une information claire, facile à trouver et à comprendre à donner aux personnes concernées avant d'évaluer si on autorise un traitement (en se basant alors éventuellement sur un opt-out plutôt que sur un opt-in). Par ailleurs, d'autres contributeurs soulignent qu'il faut se méfier des *privacy policies* longues et rarement lues. Pour l'APEP-Association Professionnelle Espagnole de la Vie privée- on devrait introduire un devoir général d'information dans le but d'assurer la transparence.
68. La European Newspaper Publishers Association et la FAEP (European Federation of Magazine Publishers) signalent qu'une exemption pour les médias serait nécessaire pour toute question de consentement, que ce soit en termes d'obligation de transparence et

d'information ou comme une condition nécessaire à un traitement loyal et licite. Cela doit valoir pour toutes leurs activités : archivage d'articles, enregistrement de matériel de recherche pour préparer les articles, rassemblement quotidien d'informations, investigation, vérification, édition, suppression, que cela conduise ou non à la publication des matériaux, et enfin publication et communication ultérieure.

9. La Convention 108 devrait-elle aborder la question de la légitimation des traitements de données comme le fait la Directive 95/46 dans son article 7 ?

69. Certains contributeurs craignent que l'introduction d'une telle liste réduise la flexibilité de la Convention (TechAmerica). Le Garante, à l'instar du Commissioner for Personal Data Protection de Chypre et de CEA Insurers of Europe, souligne qu'il faut éviter de modeler de façon trop proche les principes de la Convention sur ceux établis dans la directive 95/46, ce qui conduirait à introduire des dispositions excessivement détaillées dans la Convention. Cette préoccupation est partagée par la German Insurance Association qui plaide pour un haut degré d'abstraction de la Convention, surtout en ayant en tête le souhait d'adhésion de pays tiers. Dans la même ligne, la FEDMA indique que cela ne devrait pas figurer dans le contenu d'une convention internationale. C'est davantage l'objet d'une directive.
70. Privacy International est plus radical encore. Ils estiment qu'une telle approche de la légitimité est tautologique et inutile. Ainsi, des finalités malhonnêtes sont de toute évidence non légitimes, à moins qu'elles le soient (sic) (hypothèse où l'on vise à tromper un escroc, par exemple). Pour eux, le catalogue des raisons de légitimation des traitements présent dans la directive a créé un terrain de jeu pour juristes plein de trous à éviter. Enfin, ils craignent qu'une liste de fondements positifs pour effectuer un traitement de données soit inévitablement incomplète. La combinaison de l'exigence de loyauté et licéité (« lawful (i.e. not unlawful) »), couplée aux autres principes généraux de proportionnalité, minimisation des données et collecte non intrusive, représente à leurs yeux des critères appropriés. Ces derniers points sont repris textuellement par le Cyberspace Law and Policy Centre et par le consortium CLSR-IAITL-ILAWS.
71. Aux antipodes, certains répondants trouvent opportun, utile voire important d'insérer une telle liste de fondements légitimes, par souci de cohérence avec le droit de l'UE ou par souci de clarté pour les acteurs de terrain qui ont besoin de disposer de paramètres clairs à propos des traitements licites (AEDH, European Privacy Association, European Banking Federation, Data Industry Platform, the CZECH Office for Personal Data Protection, la Commission pour la protection des données personnelles de Bulgarie, la Direcçao Geral da Politica de Justiça du Portugal, le Ministère de la Justice du Royaume-Uni). EFAMRO et ESOMAR accueillent favorablement l'introduction d'un fondement pour le traitement légitime des données dans la Convention mais ne sont pas en faveur d'une liste exhaustive de fondements légitimes.

10. La Convention 108 ne fait pas de référence expresse à la compatibilité nécessaire entre l'utilisation des données et le but initial de leur collecte. Or, aujourd'hui, les données à caractère personnel sont généralement utilisées à des fins qui vont bien au-delà de celles initialement prévues, d'où la question de la compatibilité.

72. Peu de répondants ont compris la pertinence de cette question étant donné que l'article 5 de la Convention exige déjà que les données ne soient pas utilisées de façon incompatible avec les finalités. Pour beaucoup la question est donc déjà réglée.
73. Certains notent toutefois que la question des traitements ultérieurs est de plus en plus fréquente, surtout dûe à la disponibilité massive des données sur le Net, et devrait être traitée.
74. Pour la European Privacy Association, la question principale n'est pas de mentionner l'exigence de compatibilité avec le but mais plutôt d'étendre l'application de l'article 5, b) de la Convention à tout traitement de données. Ils suggèrent de prendre pour modèle le texte de l'article 6, 1, b) de la directive.
75. Il est relevé qu'il faudrait permettre les traitements ultérieurs à des fins historiques, statistiques ou scientifiques. EFAMRO et ESOMAR demandent que la recherche de type « market, social and opinion research » ne soit pas considérée comme incompatible avec la finalité initiale d'un traitement de données, ce qui est déjà admis dans la recommandation R(97)18. Ces acteurs demandent qu'une disposition semblable à l'article 6, paragraphe 1.b) de la directive 95/46 soit intégrée dans la Convention.
76. CEA Insurers of Europe demande qu'il soit possible de changer de but, dans les cas où l'on peut justifier légalement le nouveau but.
77. Matthias Pocs, se penchant sur cette question au sein du secteur de la police où la question se pose avec acuité, propose, en étayant sa proposition de développements circonstanciés, que la Convention 108 prévoie que le traitement de données à caractère personnel pour des finalités différentes de celles spécifiées soit interdit si la personne concernée est suspectée d'une forme d'infraction peu grave ou modérément grave, mais qu'il soit autorisé si la personne concernée est suspectée d'une forme grave de crime et que des garanties adéquates contre les violations de la dignité humaine soient apportées.

11. La définition des catégories particulières de données faisant l'objet d'une protection accrue est très large, ce qui pourrait entraîner une application excessive de cette restriction : est-ce l'information ou son traitement qui est sensible ? Devrait-on ajouter d'autres catégories de données, comme les numéros d'identification (nationaux) et les données biologiques ou biométriques ?

78. **La pertinence d'une catégorie de données sensibles** : Le ministère de la justice britannique invite le Comité consultatif à réfléchir à ce que les données sensibles pourraient être liées à leur usage plutôt que simplement étendre la liste des données sensibles (il renvoie à l'exemple d'une photographie qui pourrait être considérée comme donnée biométrique et pour laquelle il y a une immense différence entre être reprise sur une carte de bibliothèque et être prise à la sortie d'un centre de désintoxication pour drogués). Cette position est partagée par plusieurs contributeurs pour qui la sensibilité des données est essentiellement contextuelle.

79. Pour plusieurs contributeurs, le principe de proportionnalité offre des garanties adéquates pour ces données. On pourrait ne pas toucher à la liste actuelle et reposer sur le principe de proportionnalité pour faire face aux dangers liés à d'autres données.

80. Pour le Garante italien, il ne faudrait pas toucher à la protection accrue offerte aux données figurant dans la liste actuelle, qui correspond grosso modo aux catégories protégées par les instruments internationaux pour lutter contre les discriminations. Par contre, on pourrait envisager un critère « fonctionnel » par lequel des catégories additionnelles de données pourraient être considérées comme sensibles à cause du contexte et/ou de la finalité et/ou des mécanismes de leur traitement. Dans ces cas, ces données seraient sujettes à une protection accrue. On pourrait également envisager que les circonstances et catégories de données puissent être déterminées et mises à jour régulièrement par des outils flexibles qui n'impliquent pas des amendements à la Convention. Cette position du Garante rejoint celle du Commissaire à la protection des données de l'Ile Maurice pour qui on pourrait distinguer les données sensibles du fait de leur nature et celles qui le sont du fait du traitement qui leur est appliqué (comme le nom ou la photo qui font apparaître l'origine raciale). L'APEP insiste aussi sur le fait que les dommages qui peuvent résulter du traitement de ces données sensibles dépend de la finalité du traitement.

81. **La liste des données sensibles** : plusieurs contributeurs s'interrogent sur ce que recouvre la notion de données « biologiques ». Pour certains cela ne devrait pas recouvrir des caractéristiques comme le genre et l'âge, visibles aux yeux de tout le monde.

82. Certains suggèrent l'introduction des données génétiques et biométriques dans la liste.

83. SAFRAN-groupe MORPHO, société spécialisée dans l'identification et dans les applications utilisant la biométrie, précise qu'à l'inverse du nom, les empreintes digitales ne donnent aucune indication sur l'origine ethnique ou sur l'appartenance à une religion supposée. Le nom est en outre la clé d'accès à des tas de données sur Internet par l'intermédiaire des moteurs de recherche, contrairement aux empreintes digitales. Cette société s'interroge donc : pourquoi soumettre les données biométriques à un régime juridique plus contraignant alors qu'elles fournissent moins d'informations que le nom des gens ? Par ailleurs, SAFRAN s'interroge sur le sort à réserver aux « empreintes vocales » récoltées par des systèmes de messagerie et stockées sur des serveurs pour constituer des bases de données biométriques. Ces données doivent-elles bénéficier d'un régime juridique différent des empreintes digitales et sur quel fondement ? Apportant encore des précisions sur les empreintes génétiques à distinguer des données génétiques, ce répondant signale que dans certaines situations l'utilisation de données biométriques comme l'iris ou l'empreinte digitale, anonymisées, permet de déterminer si un individu peut se voir ou non accorder un droit (d'entrer par exemple) sans que son identité ne soit dévoilée.

84. L'APEP-Association Professionnelle Espagnole de la Vie privée partage cette réticence à voir les données biométriques considérées comme sensibles, étant donné qu'en principe ces données ne révèlent pas d'informations sur la santé. Pour cet organisme, il est également difficile de considérer les numéros d'identification (nationaux) comme sensibles.

85. Pour l'AEDH, mises à part les informations biologiques nécessaires dans un contexte médical, il y a lieu de s'interroger si, au nom de la protection de la personne humaine, des informations telles que les identifiants nationaux et les données biologiques ou biométriques, qui servent donc d'identifiants sûrs d'une personne, devraient tout simplement exister, surtout quand elles concernent tous les membres d'un peuple et non certaines personnes pour des motifs particuliers au regard d'une nécessité publique. Pour cet organisme, l'existence de tels systèmes d'information est très dangereuse dans toutes circonstances exceptionnelles (régime devenant non démocratique). En outre, ces systèmes d'attachement physique des personnes à l'Etat rompt le contrat social et repose sur l'idée que tout citoyen est un délinquant potentiel, ce qui n'est pas acceptable. Ce n'est

donc pas un régime de protection renforcée pour prévenir les discriminations comme dans le cadre des données sensibles qui doit être réservé à de telles données. C'est un régime d'interdiction qui ne peut être levé que sur la base des critères énoncés à l'article 9 de la Convention.

86. La CNIL propose d'évoquer l'origine ethnique plutôt que l'origine raciale.
87. Plusieurs répondants demandent que si l'on songe à étendre la liste des données sensibles, cela soit précédé d'une étude d'impact.
88. Quant au **régime de ces données**, la CNIL demande qu'il soit plus détaillé car ce qui se trouve actuellement dans la Convention manque de précision. Cette autorité indique aussi qu'il faudrait une exemption pour les traitements statistiques et la recherche scientifique.
89. EFAMRO et ESOMAR souhaitent quant à eux que l'on apporte des clarifications sur la portée de ce qui constitue des données sensibles. Ils pointent également qu'imposer le recours à une autorité avant de permettre de traiter des données sensibles est une charge trop lourde et une entrave trop importante pour le secteur de la recherche.
90. La European Newspaper Publishers Association et la FAEP demandent une exemption pour le secteur de la presse par rapport au régime strict réservé aux données sensibles.

12. Une protection spécifique pourrait également être appliquée à certaines catégories de personnes sur lesquelles portent les données. Les enfants, en particulier, peuvent avoir besoin d'une protection spéciale en raison de leur vulnérabilité. Y-a-t-il un besoin de dispositions spécifiques à la protection des enfants ? Si tel est le cas, quels aspects devraient aborder ces dispositions ?

91. Les données relatives aux mineurs ne devraient pas tomber dans la catégorie des données sensibles étant donné que la personne concernée par les données ne peut être un critère de sensibilité (Commission pour la protection des données personnelles de Bulgarie).
92. Cela étant dit, il importe de prévoir des conditions particulières pour protéger les mineurs à cause de leur vulnérabilité. Cela semble nécessaire à plusieurs répondants. L'APEP-Association Professionnelle Espagnole de la Vie privée relève que tout le monde est d'accord pour dire que les enfants méritent une protection spécifique mais que le débat porte sur l'âge pertinent à prendre en considération, si et à partir de quand le contrôle parental porte atteinte au droit de l'enfant à la vie privée, qui doit octroyer l'autorisation parentale,… Pour cette association, des obligations spécifiques devaient être imposées dans les hypothèses où les enfants sont la cible du traitement. Le régime de protection spécifique devrait être basé sur des obligations de moyens et non de résultat.
93. La Federal Trade Commission présente le régime légal américain spécifique de protection des enfants en ligne (le Children's Online Privacy Protection Act) qui prévoit une série de règles visant à protéger les enfants de moins de 13 ans. Ce régime est en phase de révision pour s'assurer qu'il répond toujours adéquatement à l'évolution des technologies et surtout des pratiques qui a vu exploser l'usage des terminaux mobiles et des jeux interactifs par les enfants.
94. Par contre pour de nombreux autres, un régime de protection particulier n'a pas sa place dans la Convention. D'autres textes offrent un régime spécifique. Une recommandation serait sans doute plus appropriée en la matière. Ou, le rapport explicatif pourrait clarifier que l'introduction des principes de proportionnalité et de minimisation sont une réponse

adéquate aux préoccupations concernant les enfants – ainsi que d'autres groupes vulnérables (CLPC, Australie).

95. D'autant qu'il y a des difficultés à harmoniser ce qu'il faut entendre par mineur, mineur avec capacité de discernement et mineur avec capacité d'exprimer un consentement. De même qu'il y a des difficultés à faire respecter et contrôler des limites d'âge sur Internet.

96. Enfin, plusieurs contributeurs signalent qu'il y a d'autres catégories de personnes vulnérables que les mineurs.

13. L'article 7 de la Convention porte sur la sécurité des données au sens restrictif du terme, à savoir la protection contre la destruction accidentelle ou non autorisée, la perte accidentelle et l'accès non autorisé, la modification ou la diffusion. La notion de sécurité devrait-elle également inclure un droit pour les personnes concernées d'être informées des violations de la sécurité des données ?

97. Pour de nombreux répondants, il serait opportun de prévoir un tel droit à être informé des violations de sécurité, applicable de façon horizontale au sein de tous les secteurs. Pour le CLPC ainsi que pour le consortium CLSR-IAITL-ILAWS et pour Privacy International, ce droit ne devrait d'ailleurs pas paraître comme partie du principe de sécurité mais comme un principe séparé.

98. Il est impératif pour la plupart de baliser clairement les limites d'un tel droit. European Privacy Association précise qu'il faudrait indiquer quand l'information devrait être donnée, à qui et de quelle manière. TechAmerica Europe propose des balises pour définir cette obligation. La Commission à la protection des données du Sénégal estime qu'il faut obliger à informer les autorités publiques de contrôle mais non les personnes concernées qui ne pourront de toute manière rien faire face aux violations. La German Insurance Association apporte l'éclairage de l'expérience allemande : en 2009, un amendement de la législation allemande de protection des données a introduit un devoir d'informer en cas d'accès non autorisé aux données. Cette obligation s'applique si des données particulièrement sensibles sont affectées et s'il y a un risque réel d'atteinte sévère aux droits ou aux intérêts légitimes des personnes concernées. A leur connaissance cette règle a suscité une expérience positive. Ils insistent sur la nécessité de limiter ce genre d'obligation aux seuls cas de risque réel pour les personnes concernées. Morpho-groupe Safran ne se penche pas sur les hypothèses d'accès non autorisés mais estime que ce droit à être informé des violations de sécurité devrait être expressément justifié par la nécessité de protéger l'identité et de limiter les risques d'usurpation d'identité.

99. Toutefois, plusieurs répondants craignent qu'il ne soit pas possible d'introduire un tel droit sous peine de transformer la Convention en instrument trop détaillé et non restreint à des principes généraux.

100. Certains répondants, comme l'Office de protection des données personnelles de la République tchèque, sont opposés à l'idée d'introduire ce droit estimant que la question est suffisamment traitée au sein de la directive européenne. La Data Industry Platform craint qu'on n'impose des charges additionnelles sur les acteurs de terrain sans apporter aux personnes concernées un plus haut niveau de protection. Ce groupe de signataires comprend l'importance de la sécurité et de la nécessité de créer la confiance entre les personnes concernées et les responsables de traitement. Ils trouvent donc le concept « sympathique » dans la mesure où c'est un incitant à la sécurité. Ils estiment toutefois que la question serait plus adéquatement adressée par des instruments d'autorégulation. La FEDMA et la European Banking Federation ont formulé exactement les mêmes craintes et convictions. EMOTA (European E-commerce and Mail Order Trade Association) partage également ces doutes.

101. Plusieurs ont indiqué qu'il ne fallait en tout cas pas tomber dans une formule « *overly prescriptive* » qui conduirait à une charge excessive et enlèverait en même temps son efficacité à la mesure, banalisant les notifications auprès des intéressés.

102. Pour le Garante italien la question de la sécurité est devenue une question cruciale, surtout dans le contexte du *cloud computing*. L'article 7 de la Convention devrait être revu. Il serait approprié d'envisager d'étendre le concept de sécurité pour inclure la sécurité des réseaux de transmission de données en sus de la sécurité physique des locaux où les données sont conservées.

103. Dans le même sens, Privacy International recommande que l'on passe d'une « sécurité des données » interprétée passivement à une obligation positive de concevoir les systèmes pour minimiser le risque pour la vie privée – par exemple par une minimisation ex ante. Il ne faut donc pas seulement veiller à protéger les données qui sont traitées mais à minimiser le risque pour la vie privée du système tout entier.

14. Il existe certains risques découlant de l'utilisation des données de trafic et de localisation (données techniques accompagnant une communication) car ces données peuvent révéler les mouvements, orientations, préférences et associations avec d'autres. Avons-nous besoin de règles particulières pour l'utilisation de ce type de données ?

104. Les réponses à cette question sont contrastées.

105. Certains estiment que ce serait opportun de prévoir un régime de protection renforcée pour les traitements visant à localiser les individus dans l'espace.

106. L'AEDH précise que les données de trafic mettent en jeu la liberté de communication, et les données de localisation la liberté d'aller et venir. De par cette interférence sur des libertés, un régime plus strict devrait leur être appliqué. Il en est de même pour les requêtes formulées sur un moteur de recherche qui mettent en jeu la liberté d'information. Dans le même sens, pour Privacy International, les données de trafic et de localisation sont des données concernant les relations sociales et empiètent sur la liberté d'association et sur le droit de s'associer librement de manière privée et non observée. En conséquence, pour Privacy International, de telles données doivent constituer une catégorie spéciale et devraient être considérées comme intrinsèquement « toxiques » pour la vie privée.

107. La CNIL signale que faire entrer ces données dans la catégorie des données sensibles risque de conduire à placer un frein à certaines innovations techniques. Il serait préférable plutôt d'ajouter des éléments de protection clairement distincts dans la Convention visant notamment à imposer des garanties appropriées pour « les données à caractère personnel utilisées dans des traitements ayant pour finalité de révéler la position dans l'espace d'un individu ». Cela permettrait d'exclure les données qui peuvent révéler la localisation d'un individu mais dont ce n'est pas la finalité tout en ne faisant pas entrer ces données dans les données spéciales visées à l'article 6 de la Convention. Une troisième option possible présentée par la CNIL serait de proposer un droit spécifique à ne pas être géo-localisé.

108. Pour d'autres répondants, il n'est pas nécessaire de prévoir un régime spécifique. L'Information Commissioner britannique, pour sa part et dans le même sens, estime que la sensibilité tient davantage dans le traitement des données et les effets qu'il peut avoir sur les individus que dans la nature des données traitées.

109. Pour le CLPC, appuyé par le CIPPIC, il ne devrait pas y avoir besoin d'un régime particulier si l'on veille à faire entrer les données de trafic et de localisation dans la définition des données à caractère personnel en prévoyant expressément que les données à caractère personnel englobent toute information qui permet ou facilite la communication avec une personne sur une base individualisée, que cette information rencontre ou non l'actuelle définition de donnée à caractère personnel.

15. Faut-il mettre en place des systèmes de responsabilisation, ainsi qu'une obligation de prouver que des mesures efficaces ont été prises pour garantir le plein respect de la protection des données ?

110. La plupart des répondants qui se sont prononcés sur cette question approuvent l'idée d'introduire une obligation de respect du principe « d'*accountability* », comme garantie d'amélioration de la protection offerte. Les mécanismes d'*accountability* devraient être clairement définis, non excessifs et mis en œuvre de la même façon parmi les signataires.

111. Privacy International, de même que le consortium CLSR-IAITL-ILAWS, invitent à se montrer prudent par rapport à la suggestion faites par certains de voir l'*accountability* comme une alternative à l'exigence de respect des règles de protection. L'*accountability* ne peut devenir une alternative aux restrictions d'exportation de données. Cette organisation est préoccupée à propos des conséquences ou plutôt de l'absence de conséquences que des failles au niveau de l'*accountability* peuvent avoir si ce principe est interprété de façon laxiste.

112. L'APEP-Association Professionnelle Espagnole de la Vie privée estime pour sa part qu'il faudrait octroyer une « récompense » (une réduction de sanction, par exemple) pour les responsables de traitements « *accountable* » dans les hypothèses où les violations de la protection des données sont dues seulement à une erreur exceptionnelle.

113. TechAmerica Europe soutient l'introduction d'un principe d'accountability s'il est défini dans une approche ex post basée sur l'application des règles plutôt que dans une approche ex ante basée sur la conformité aux règles. Dans un régime ex post, les organisations sont responsables de ce qu'elles font avec les données où que celles-ci aillent, au lieu de chercher simplement à être en règle avec la loi. Cela a

des implications sur comment l'organisation considère la protection des données, comment elle la met en œuvre et comment elle la supervise.

114. Certains répondants s'opposent à l'idée d'introduire une obligation de démontrer la conformité car cela représenterait une charge, spécialement pour les PME.

16. Devrait-on appliquer le principe du « respect de la vie privée dès la conception » (Privacy by Design) qui vise à prendre en compte la question de la protection des données dès le stade de la conception d'un produit, d'un service ou d'un système d'information ?

115. Il semble cohérent, au vu du fait que le principe de *Privacy by design* a été proclamé dans différentes enceintes, a fait l'objet d'une résolution adoptée par la 32eme conférence internationale des autorités de protection des données et est pris en considération par la Commission européenne dans le cadre de la révision de la directive 95/46, que ce principe soit également consacré par la Convention 108 (SAFRAN).

116. D'autres répondants partagent la conviction que ce principe devrait être expressément encouragé, même s'il sera difficile de l'opérationnaliser en une règle spécifique (Privacy International, Ministère de la Justice britannique, CNIL, Commission à la protection des données du Sénégal). Ou qu'il est bienvenu mais qu'il faudrait clarifier bien davantage comment il sera défini ou mis en œuvre avant de pouvoir véritablement le soutenir (TechAmericaEurope). L'introduction du principe de *Privacy by design* favoriserait une approche proactive de la protection plutôt que de reposer exclusivement sur des mesures de redressement (Garante). Pour l'AEDH, l'obligation d'appliquer les principes de protection dès la conception des équipements et des applications pourrait être simplement précisée dans le texte, sans forcément recourir à une « vocabulaire marketing » tel celui de *privacy by design*. Pour le ICUK, ce principe se trouve implicitement dans les principes de protection existants. Toutefois, une exigence explicite aurait l'avantage de donner un signal clair aux concepteurs de systèmes d'information, à ceux qui les approvisionnent et à ceux qui les font fonctionner.

117. Le Garante italien précise toutefois que l'efficacité du principe ne pourra être assurée qu'en spécifiant comment son impact sur les opérations spécifiques du traitement peut ou devrait être mesuré et par qui, à la lumière de dispositions technologiques spécifiques.

118. La Commission pour la protection des données personnelles de Bulgarie estime que pour une application effective de ce principe il faudrait prévoir l'obligation pour les responsables de traitement d'effectuer des évaluations de risque pour la vie privée lors du traitement de données. Privacy International est également favorable à une obligation d'effectuer des « privacy impact assessment » pour les projets majeurs.

119. Pour cette dernière organisation, le moyen le plus simple d'exprimer le principe de *privacy by design* consiste à dire que si des découvertes scientifiques démontrent qu'un service peut être offert pratiquement par une voie plus respectueuse de la vie privée, l'adoption de technologies protectrices de pointe peut être imposée. Ils relèvent encore qu'il ne faut pas être influencé par la fausse rhétorique des lobbyistes qui tentent de cantonner la *privacy by design* à un simple état d'esprit attentif aux principes de protection des données lors de la conception des produits commerciaux, « immunisant » le concept de toutes obligations techniques.

120. Pour TechAmerica Europe, la *privacy by design* est un processus que les organisations devraient suivre au début d'un projet et réévaluer régulièrement pour assurer que les mesures de protection des données et de sécurité demeurent appropriées. Il est important que quelle que soit l'exigence introduite dans le texte légal, cela reste de l'ordre des procédures et non de la technologie. Pour AFME BBA (monde bancaire), la formulation du principe doit être de haut niveau et non prescriptive quant aux mesures qui devraient être adoptées.

121. La FTC a pour sa part recommandé dans son rapport destiné à améliorer la protection de la vie privée aux Etats-Unis que les entreprises adoptent une approche « *privacy by design* ». Ceci implique de construire des protections pour la vie privée au sein des pratiques journalières des affaires. Ces protections incluent l'offre d'une sécurité raisonnable pour les données à caractère personnel, la limitation de la collecte de données aux seules données nécessaires et la conservation des données durant une période limitée. Sur la base de son expérience, la FTC encourage le Comité consultatif de la Convention 108 à retenir le concept d'adaptabilité en abordant la question de *privacy by design*.

Droits – Obligations

17. Le droit d'accès ne devrait pas se limiter aux données mais devrait couvrir l'accès à l'origine des données, c'est-à-dire la personne qui est à l'origine de la communication. Ce droit devrait-il également couvrir l'accès à la logique du traitement ?

122. L'ajout du droit d'accès à l'origine des données et à la logique qui sous-tend un traitement est absolument nécessaire aux yeux de l'AEDH, très importante, pour la Commission bulgare, permet la cohérence avec le régime de l'UE, pour le ICUK et le Ministry of Justice britannique, s'impose dans le contexte grandissant des modèles informatiques complexes sur lesquels on base des critères et des suppositions et qui peuvent avoir un effet négatif sur la sphère privée des individus, pour le CIPPIC et le Garante, et doit tout simplement être envisagé pour d'autres répondants. La European Privacy Association craint toutefois qu'étant donnée l'implication d'un nombre important d'intervenants dans les traitements automatisés aujourd'hui, l'obligation de transparence du processus de traitement – que cette association soutient – ne soit plus réalisable sans supporter des coûts excessifs.

123. L'AFME et BBA (banques) soutient l'initiative pourvu que cela ne dépasse pas le droit instauré par la directive 95/46, dans la mesure où cela ne reviendrait pas à obliger les acteurs à conserver des informations sur les sources des données, mais ne représente qu'un devoir de transmettre les informations sur les sources si celles-ci sont connues. Sur le point de la conservation des informations sur les sources des données, la réponse de la German Insurance Association indique que la loi allemande de protection des données impose l'obligation de conserver les données sur les sources et sur les destinataires des données durant une période de deux ans.

124. La Direcçao Geral da Politica de Justiça du Portugal estime que l'accès à la logique du traitement nécessite pour le sujet des données de démontrer un intérêt et doit être limité dans la mesure stricte de la satisfaction de cet intérêt. L'accès à la logique du traitement ne doit donc pas se traduire en divulgation injustifiée de secrets d'affaires.

125. CEA Insurers of Europe relève que certaines demandes d'accès sont « frivoles » et ne visent qu'à contrôler le traitement de données plutôt qu'à vérifier l'exactitude des données traitées. En conséquence ce groupe estime que le droit d'accès devrait être limité et qu'on ne devrait pas envisager d'introduire le droit d'accès à connaître la logique dans la Convention108. Cette position est partagée par la Data Industry Platform qui est soucieuse de préserver les secrets commerciaux, la compétitivité des entreprises et leur propriété intellectuelle. Les techniques internes d'analyse prédictive sont une valeur cruciale pour le monde des affaires et ne devraient pas être révélées à des tiers. La FEDMA rejoint cette position.

126. Privacy International estime que la protection offerte à la propriété intellectuelle (brevets) permet d'être transparent sans crainte. Dans les cas exceptionnels où le secret doit être préservé, il faudrait que les autorités de contrôle puissent inspecter confidentiellement les algorithmes pour en vérifier la légitimité.

127. La FTC fournit des indications de cas dans lesquels aux Etats-Unis les consommateurs ont le droit d'obtenir des informations des entreprises qui ont pris des actions ayant un effet négatif sur eux. Un cas illustre que l'on peut atteindre un compromis entre transparence et secret des affaires : les agences de credit reporting ne sont pas tenues de révéler précisément comment les scores de crédit sont calculés, mais la divulgation qu'elles doivent effectuer doit inclure l'éventail des scores de crédits possibles dans le modèle d'évaluation et les facteurs clés qui ont affecté négativement le score du consommateur.

128. La CNIL insiste pour que l'exercice des droits d'accès, d'opposition, de correction et blocage se fasse gratuitement.

129. Le Garante invite à réfléchir, concernant les technologies basées sur le cloud computing, à introduire un droit de connaître la localisation physique et le pays où la conservation des données ou les serveurs de distribution sont situés.

18. Le droit d'opposition se justifie dans les cas où le traitement des données ne repose pas sur le consentement de la personne concernée. Le lien entre droit d'opposition et droit à l'oubli pourrait être examiné, ainsi que la possibilité de garantir le respect et l'exercice de ce droit.

Le droit d'opposition

130. Le droit d'opposition se justifie aux yeux de la plupart des répondants, mais pas en toutes circonstances. On pourrait songer à introduire ce droit dans la Convention par souci de cohérence avec la directive. A l'inverse de certains répondants, d'autres estiment que ce droit devrait être accordé même lorsque le traitement se fonde sur le consentement, s'il est admissible que le consentement soit révocable en toutes circonstances.

131. Un droit proche existe dans la loi canadienne (PIPEDA), permettant aux personnes concernées de s'opposer par opt-out aux finalités non nécessaires pour la collecte, l'utilisation et la communication des données à caractère personnel.

132. La Commission bulgare a souligné que le lien entre le droit d'opposition et le droit à l'oubli consiste en ce que le droit d'opposition s'exerce en tenant compte de la finalité du traitement, tandis que le droit à l'oubli s'exerce au-delà de la question d'une justification du traitement au regard de la finalité.

Le droit à l'oubli

133. Il ressort de la plupart des réponses ce qui suit. Le droit à l'oubli peut être particulièrement indiqué et praticable dans certaines circonstances (essentiellement dans le cadre des réseaux sociaux). Pour le reste, il est problématique sur plusieurs points :

134. - il entre en conflit avec les droits, intérêts et libertés d'autrui, notamment la liberté d'expression, la liberté de la presse (il empiète sur la conservation d'archives complètes), le devoir de mémoire, la continuité des affaires, la gestion des dossiers des employés, le devoir de conserver les preuves… Il est une entrave à la recherche historique. Il peut également entraver la fourniture de certains services comme les soins médicaux au cas où il n'y a plus connaissance du passé médical de la personne concernée ;

135. - il est difficile à mettre en œuvre une fois que les données ont été rendues publiques sur internet.

136. Pour l'APEP, le droit à l'oubli n'est pas une sous-catégorie du droit d'opposition dans la mesure où, à la différence de ce dernier, il a un effet rétroactif. La question est donc, pour cet organisme, de savoir si les individus doivent être responsables sine die de leurs actions passées et s'il est souhaitable qu'ils aient le droit de réécrire leur passé, et donc aussi le passé des autres.

137. Certains répondants soutiennent son insertion dans la Convention. D'autres, plus nombreux, estiment qu'il faut approfondir la réflexion avant de se prononcer, notamment en se penchant sur les obstacles pratiques à sa réalisation et en éclaircissant le coût et les implications concrètes induits par un tel droit. Des éclaircissements sur les données qui seraient l'objet d'un tel droit d'effacement devraient aussi être apportés : si cela concerne les données provenant de la personne concernée, cela couvre-t-il aussi les données d'analyse ou méta-données créées par le responsable du traitement ? On souligne que le droit à l'oubli ne peut en tout cas pas être absolu. La Data Industry Platform relève que ce droit ne devrait pas figurer dans un catalogue de principes généraux et éprouvés dans la durée. Sur ce point elle est appuyée par le Garante qui ne voit pas d'un bon œil l'insertion d'un droit aussi controversé dans la Convention.

138. Pour la Data Industry Platform, si l'on devait envisager l'insertion de ce droit, il faudrait impérativement le limiter aux services basés sur des données que les individus concernés ont eux-mêmes fournies et qui sont rendues accessibles à des tiers comme objet du service. Certains répondants rejoignent cette position, limitant le champ d'application d'un tel droit aux réseaux sociaux.

139. Pour d'autres répondants, enfin, ce droit est carrément irréaliste sur les plans technique et légal (EMOTA- European E-commerce and Mail Order Trade Association) ou aurait des conséquences désastreuses pour les éditeurs et la liberté d'expression (European Newspaper Publishers Association et European Federation of Magazine Publishers) et devrait absolument être rejeté (notamment les différents intervenants du monde de la presse).

19. Devrait-il y avoir un droit qui garantisse la confidentialité et l'intégrité des systèmes d'information ?

140. Il est à noter que d'assez nombreux répondants ont omis de répondre à cette question.

141. Pour certains répondants la réponse est positive, la plupart du temps non étayée. Parmi ceux-ci, le Garante italien se démarque en exprimant que, pour lui, les droits en cause à cette question, de même que ceux en jeu dans les deux questions suivantes, sont ceux qui justifient le plus d'étendre la liste des droits et des principes généraux de la Convention.

142. Mais d'autres répondants ne voient pas en quoi la confidentialité et l'intégrité des systèmes devraient faire l'objet d'un droit, plutôt que de renforcer les contraintes de sécurité de l'article 7. La plus-value d'un tel droit resterait à démontrer et devrait être confrontée au risque de dilution et de perte de lisibilité des droits figurant dans la Convention.

143. L'Office pour la protection des données personnelles tchèque précise que la garantie de confidentialité se rattache aux obligations pesant sur le responsable et non aux droits.

20. Faudrait-il introduire le droit de tout individu à « ne pas être localisé / tracé» (identification RFID) ?

144. Certains répondants sont d'accord à l'idée d'introduire un tel droit, mais avec des exceptions raisonnables.

145. Rappelons la remarque du Garante formulée à propos des trois droits en cause aux questions 19, 20 et 21, qui estime ce droit crucial.

146. Pour d'autres, ce droit nécessite une réflexion plus approfondie.

147. L'AEDH et la Data Industry Platform pensent que l'application des principes généraux de protection (notamment l'interdiction de conservation des données au-delà de l'objectif) offre une réponse satisfaisante. Le CIPPIC, dans le même sens, estime que les principes « de confidentialité, de vie privée et d'exactitude » réalisent ce droit. Le CLPC, quant à lui, estime également qu'il n'y a pas besoin de consacrer un droit séparé si l'on définit les données à caractère personnel de manière à englober les informations à propos des communications, de la localisation ou du comportement d'un individu.

148. European Privacy Association suggère que plutôt que de parler d'un droit à ne pas être tracé, on mette en place une option à ne pas être tracé. Les personnes concernées devraient être informées des pratiques de traçage et se voir fournir l'option et les moyens technologiques de refuser d'être tracé/localisé. L'APEP parle également d'une option à rendre disponible aux personnes concernées, refusant l'idée d'une interdiction. Les technologies de traçages ne sont pas mauvaises en soi mais certains usages doivent être limités dans les cas où la vie privée doit l'emporter. Pour cet organisme on ne devrait pas empêcher le traçage des patients Alzheimer, des bagages perdus, des véhicules, des enfants ou des animaux. Par ailleurs le concept de traçage n'est pas limité au RFID mais couvre aussi notamment les cookies.

149. Plusieurs répondants font remarquer qu'il ne faut pas baser un droit sur une technologie ciblée, cela est contraire à l'objectif de conserver à la Convention son caractère technologiquement neutre.

150. Il ne faut pas non plus que par la législation on empêche tout progrès et tout développement technique en la matière.

21. Les utilisateurs des technologies de l'information et de la communication devraient-ils avoir le droit de rester anonymes ?

151. Rappelons la remarque du Garante formulée à propos des trois droits en cause aux questions 19, 20 et 21, qui estime ce droit crucial.

152. L'AEDH relève que la vie sociale repose sur une dialectique de l'identification et de l'anonymat qui ne se retrouve plus dans les conditions d'aujourd'hui où par exemple, la consultation d'informations publiques laisse des traces identifiantes de même que tout paiement puisqu'il n'y a pas de monnaie électronique équivalant aux billets de banque. Cela constitue un « vice de base ». Tout repose dans un tel contexte sur la durée de conservation des données collectées. Il faudrait, aux yeux de cette association, garantir socialement et techniquement un droit à l'anonymat.

153. Dans la même ligne, le CIPPIC est d'avis que l'anonymat est un droit qui mérite une formulation et une protection distinctes. Pour ce centre, la capacité d'agir anonymement est centrale dans la protection de la vie privée dans les espaces publics et semi publics. Il signale que la formulation du principe qui est proposée par le CLPC sur la base de ce qui se trouve dans la législation australienne de vie privée est intéressante. Le CLPC propose la formule suivante : « Les individus doivent avoir l'option de ne pas s'identifier lorsqu'ils traitent avec une entité, ou d'utiliser un pseudonyme, excepté en présence d'une obligation légale d'identification ou s'il est impraticable pour l'entité de traiter avec des individus qui ne se sont pas identifiés ou qui utilisent un pseudonyme. ».

154. Plusieurs répondants sont favorables à un droit à l'anonymat tant que l'on ne viole pas la légalité.

155. Pour plusieurs commentateurs, par contre, il ne devrait pas y avoir un droit à l'anonymat car cela pourrait conduire à une augmentation de la fraude et de la criminalité, rendant difficile voire impossible la recherche des auteurs. La European Privacy Association s'oppose à un droit générique à être absolument anonyme lorsqu'on utilise les TIC, qui serait contraire aux nécessités pratiques (les citoyens ont besoin d'information sur leur utilisation des TIC, à tout le moins pour l'établissement de factures liées à cette utilisation) et aux besoins des services de lutte contre la criminalité. Par contre ces informations doivent être protégées contre les usages abusifs. Pour la EPA, cette protection est déjà assurée par la Convention. L'APEP donne l'exemple de la surveillance légitime par le patron des actions de ses employés dont il sera rendu redevable.

156. La Data Industry Platform, à l'opposé de ce qui a été relevé ci-dessus, demande si le monde hors ligne connaît vraiment des mécanismes par défaut ou un droit de demeurer anonyme dans les circonstances normales de la vie. Ainsi, le personnel d'une bibliothèque publique connaît les utilisateurs de cette bibliothèque ainsi que leurs préférences de lecture… Ce groupe ne voit aucune raison pour faire une distinction entre le monde en ligne et le monde hors ligne.

22. La Convention 108 devrait-elle aborder la question du juste équilibre entre la protection des données à caractère personnel et la liberté d'expression (nouveau concept de la presse et du journalisme dans le contexte du Web 2.0.) ?

157. Oui en général mais les répondants sont nuancés sur la manière.

158. Pour la European Privacy Association, il conviendrait d'établir le lien existant entre le droit à la protection des données et la liberté d'expression, lien décisif. Un lien avec l'article 10 CEDH pourrait être abordé dans les considérants de la Convention 108.

159. Pour l'Union européenne de Radio-Télévision (EBU-UER), l'article 9, 2, b) accompagné du point 58 du rapport explicatif n'est pas suffisant et devrait être explicitement renforcé pour donner une exemption claire de l'application de certaines règles de protection des données pour les activités de journalisme, en particulier dans le champ audiovisuel. Cet organisme propose en conséquence d'amender l'article 9 en ajoutant un alinéa qui stipule : « 9, 2, c) protéger le traitement de données à caractère personnel effectué exclusivement à des fins journalistiques ». Une telle modification est vitale aux yeux de l'UER afin de préserver la liberté des médias, le journalisme d'investigation et la confidentialité des sources journalistiques.

160. Le Centre for Socio-Legal Studies propose quant à lui de rédiger une nouvelle disposition qui enjoint les Parties signataires de présenter un équilibre entre l'intérêt fondamental de la liberté d'expression et les valeurs que la protection des données tend à protéger. La disposition devrait en outre indiquer la nécessité d'adopter des exemptions larges, mais non absolues, des règles de protection au bénéfice de ces activités. Quant à la possibilité d'indiquer expressément les exemptions minimum en conformité avec l'article 10 CEDH, elle nécessite d'être davantage creusée. Le rapport explicatif devrait signaler explicitement que cette disposition protégeant la liberté d'expression n'est pas limitée à la presse. En principe cette disposition devrait valoir pour toute forme d'expression publique.

161. Pour l'APEP, toute régulation dans cette matière requiert de la flexibilité : elle ne doit apporter que des critères d'orientation mais pas effectuer elle-même une évaluation générale prédéterminée. Tandis que pour la CNIL, des dispositions similaires à celles de la loi française Informatique et Libertés pourraient être intégrées dans la Convention. Cet organisme trouverait en effet utile de préciser au plan européen les exemptions et dérogations dont les traitements pourraient bénéficier. Pour le CLPC, il ne serait pas approprié que la Convention fasse elle-même la mise en balance de tous les aspects de ces intérêts contradictoires, mais elle devrait néanmoins contenir une reconnaissance de l'intérêt public de la liberté d'expression.

162. L'AEDH relève qu'il n'y a pas de consensus même en Europe sur les limites à apporter à la liberté d'expression au nom de la protection de la vie privée. Cette association prône donc une initiative visant au rapprochement des points de vue et des procédures. Cette initiative devrait être prise au sein du Conseil de l'Europe, éventuellement en relation avec l'UNESCO.

163. Le ICUK s'interroge : à l'ère du blogging, où faudrait-il tracer la ligne ? Jusqu'où les autorités de contrôle seront-elles amenées à réguler le comportement en ligne des individus ?

164. Le Garante italien est opposé, pour sa part, à ce qu'on intègre dans la Convention des dispositions qui pourraient s'avérer moins flexibles que ce qui ressort du travail jurisprudentiel effectué par la Cour européenne des droits de l'homme pour réconcilier les deux droits ou qui n'atteindraient pas le même équilibre. Pour ce qui concerne les questions liées spécifiquement au Web 2.0, il lui semble prématuré d'édicter des règles spécifiques.

Sanctions et recours

23. Devrait-on introduire des recours collectifs dans la Convention ? Faut-il examiner l'introduction d'autres mécanismes de règlement des litiges ?

165. **Recours collectifs**. Différents répondants à la consultation jugent que l'introduction de la « class action » paraît souhaitable, soit dans certains contextes spécifiques[1], soit de manière générale et qu'il en soit question, le cas échéant, dans la Convention[2]. D'autres relèvent au contraire que la généralité de la Convention ne s'y prête pas[3]. Dans le même sens, plus largement, la question des sanctions et remède devrait plutôt relever du droit national que de la Convention[4]. Certains évoquent par ailleurs que le débat relatif à la « class action » doit avoir lieu dans un contexte plus large que celui de la protection des données[5].

166. Outre ces oppositions de méthodes apparaissent certaines réticences vis-à-vis de l'introduction générale des « class actions ». Des répondants notent qu'il n'en est pas besoin[6], voire même que ce n'est pas approprié[7]. Les « class actions » n'auraient pas d'intérêt lorsque la personne concernée peut déjà bénéficier de mécanismes protecteurs la soutenant dans l'exercice de ses droits[8] (par ex., les autorités de protection des données). Le recours collectif ne serait alors utile que lorsque les autres recours sont fébriles[9], inefficaces, bref quand il y aurait un véritable intérêt concret à recourir à ce moyen[10]. D'autres relèvent que les litiges en matière de protection des données seraient propres aux individus et se prêteraient par conséquent mal au recours collectif[11]. D'autres répondants encore soulignent le risque de l'utilisation nuisible des règles de protection des données que

[1] Avis CIPPIC.
[2] Avis Czech Republic – The office for personal data protection; avis Ile Maurice-Commissariat à la protection des données; avis Ukraine-Ministry of justice ; avis United Kingdom-Information commissioner's office ; avis Direcção-General da Politica de Justica.
[3] Avis EPA ; avis Italy-Garante per la protezione dei dati personali. Différents intervenants soulignent qu'il s'agit d'une question de droit national, voy. par exemple avis Lithuania-State data protection inspectorate.
[4] Avis CEA.
[5] Avis EBF.
[6] Avis Data Industry Platform.
[7] Avis ENPA-FAEP.
[8] Avis German Insurance Association ; voy. aussi avis Techamerica Europe, où il est souligné en outre qu'il faudrait évaluer s'il y a une demande des citoyens en ce sens.
[9] Avis Italy-Garante per la protezione dei dati personali.
[10] Avis UK Ministry of Justice.
[11] Avis FEDMA.

permettraient les recours collectifs[12]. Traiter à ce stade des recours collectifs serait également source d'incertitude[13].

167. Quoi qu'il en soit, la Convention pourrait néanmoins souligner l'intérêt des « class actions », leur valeur, si elle traitait finalement de la question des voies de recours[14]. Et si l'on envisageait de recourir aux recours collectifs, il importerait avant tout d'évaluer l'impact qu'ils pourraient avoir dans le contexte européen[15].

168. **ADR**. Des répondants manifestent leur soutien au recours à des ADR[16], vus par certains comme rapides et peu chers[17]. Dans le même sens, il est parfois insisté sur l'importance que pourrait recouvrir l'autorégulation dans un régime moderne de protection des données[18]. Certains répondants soulignent que la question de la résolution des litiges par des modes alternatifs est une question qui doit toutefois être réglée par les Etats et pas dans la Convention[19]. Ce serait en outre une question qui devrait être discutée dans le contexte de l'Union européenne[20]. On pourrait imaginer que la Convention se limite à consacrer l'obligation de créer des moyens alternatifs de règlement des différends mais que la matière demeurerait réservée au droit interne[21].

169. Différents intervenants notent que s'il est décidé de recourir aux ADR, cela ne devrait en tous cas pas limiter les autres voies de recours disponibles aux personnes concernées[22]. Le recours à l'ADR ne devrait pas, en outre, être une étape obligatoire et préalable à tout recours judiciaire – ou autre mais néanmoins impliquant l'autorité publique –, comme il ne pourrait constituer le seul moyen de résolution des litiges offert aux personnes concernées[23]. En cas de recours aux ADR, il serait par exemple recommandable d'utiliser les organes d'arbitrages déjà existant pour l'application de la protection des données[24].

170. Plusieurs répondants relèvent l'importance du rôle que peuvent jouer les **autorités de protection des données** – les « *Data Protection Officers* » inclus – en matière de règlement des différends. Ainsi, certains considèrent qu'elles peuvent être chargées de traiter la résolution de litiges[25]. Elles ont à cet égard besoin de la liberté d'établir des procédures et la Convention pourrait fixer un cadre normatif à cette fin[26]. En ce sens, il serait par exemple opportun de donner aux autorités de protection des données le pouvoir d'agir *ex officio*[27]. Elles pourraient également

[12] Avis APEP.
[13] Avis EMOTA.
[14] Avis Cyberspace Law and Policy Centre ; avis CLSR-IAITL-ILAWS ; avis Privacy International.
[15] Avis CNIL ; avis UK Ministry of Justice.
[16] Avis FEDMA ; avis United Kingdom-Information commissioner's office ; avis UK Ministry of Justice .
[17] Avis FEDMA .
[18] Avis United Kingdom-Information commissioner's office .
[19] Avis commun de l'AFME et de la BBA .
[20] Avis CEA.
[21] Avis Direcção-General da Politica de Justica.
[22] Avis CIPPIC.
[23] Avis CNIL.
[24] Avis German Insurance Association.
[25] Avis GDD ; avis United Kingdom-Information commissioner's office.
[26] Avis United Kingdom-Information commissioner's office
[27] Avis German Insurance Association

avoir la possibilité d'intervenir librement devant les juridictions judiciaires et administratives lors d'instances en cours[28].

171. **Autres.** Dans un tout autre ordre d'idées, certains insistent sur l'utilité de créer des **incitants** au respect de la protection des données (par ex., une réduction graduelle des exigences administratives basées sur l'historique de l'entreprise en matière de simple respect de la protection des données, voire de surpassement des exigences normalement requises)[29].

Droit applicable en matière de protection des données

24. Doit-on envisager une règle qui déterminerait le droit applicable au traitement des données (dans les cas où différentes juridictions sont concernées) ?

172. **Généralités**. Le problème du droit applicable apparaît comme important pour de nombreux répondants recommandant à plusieurs reprises que les règles soient clarifiées, en particulier dans le contexte du « Cloud Computing » (exemple fréquemment cité). La problématique du droit applicable est parfois considérée comme un obstacle pour des organisations non basée dans l'Union européenne souhaitant y établir des opérations de traitement ; le droit européen s'appliquerait sans que cette application ne soit justifiée par un lien assez fort entre la situation des individus et le droit de l'Union[30]. Certains répondent pourtant qu'ils sont convaincus que les règles actuelles en matière de définition du droit applicable sont efficaces[31].

173. Le risque qui existe en la matière est classique en droit international privé : soit il risque d'y avoir une lacune dans la protection (aucun droit applicable), soit il pourrait y avoir cumul des réglementations applicables[32]. Deux tendances concordantes en ce qu'elles souhaitent plus d'harmonisation se présentent auprès des sondés : plus d'harmonisation des concepts et règles de fond est souhaitée, et plus de clarté est demandée quant à la détermination du droit applicable. Quant à ce dernier point, les répondants émettent diverses suggestions.

174. **Harmonisation des règles de fond.** Il est clair que l'harmonisation des réglementations nationales et une interprétation conforme de la Convention auraient un effet positif[33] dans la mesure où la question du droit applicable – pour peu qu'il soit celui d'un des Etats membres du Conseil de l'Europe – perdrait de son importance – les droits étant harmonisés. En ce sens, certains soulignent la possibilité d'une harmonisation intégrée dans un cadre le plus global[34]. La promotion de la coopération internationale, la réalisation de lignes directrices au sujet des problématiques de protection des données et les « règles entre Etats » contribueraient à résoudre les difficultés actuellement rencontrées[35]. Les définitions

[28] Avis CNIL
[29] GS1 in Europe.
[30] Avis commun de l'AFME et de la BBA.
[31] Avis Data Industry Platform ; avis FEDMA.
[32] Avis CNIL.
[33] Voy. par exemple avis Techamerica Europe.
[34] GS1 in Europe.
[35] Avis CEA.

des concepts devraient ainsi être clarifiées, tout comme leur application dans les Etats membres[36].

175. Plusieurs répondants soulignent le caractère potentiellement universel – ou mondial – de la Convention du Conseil de l'Europe et l'intérêt de la promouvoir sur le plan international, comme **standard global**[37]. D'ailleurs, la résolution de Madrid, universellement acceptée, pourrait inspirer la rédaction de certains principes de la Convention 108[38]. Ces considérations valent tant quant aux questions d'applicabilité des droits nationaux, que quant aux flux transfrontières de données ; les problématiques sont clairement liées.

176. **Règle déterminant le droit applicable à la protection des données**. La complexité de la question du droit applicable est évoquée dans certains des avis communiqués, notamment dans des contextes tels que celui du « Cloud Computing »[39]. Ainsi, certaines parties soulignent qu'il serait compliqué de trancher cette question au sein de la Convention, notamment eu égard au rôle joué par l'Union européenne en la matière[40] ; il faut se coordonner. Clairement, les réflexions doivent être poursuivies en la matière, mais peut-être que la complexité du problème nécessiterait de traiter les hypothèses au cas par cas plutôt que d'établir une règle générale sur la question.

177. Il n'empêche, de nombreux répondants pensent que la question devrait être traitée dans la Convention[41] – de manière coordonnée avec la directive 95/4642 –, ou qu'il serait en tout cas souhaitable qu'il en soit ainsi[43] [44]; c'est préférable pour la sécurité juridique. D'autres relèvent que l'intégration d'une telle disposition pourrait, le cas échéant, constituer un obstacle pour une éventuelle ratification de la Convention 108 par des Etats tiers au Conseil de l'Europe[45], alors qu'il conviendrait d'en faire un instrument attractif pour ces Etats[46]. Or la protection des données et la vie privée sont des problématiques très complexes et techniques au sein desquelles demeurent des débats politiques non résolus[47]. Des sondés notent que la Convention devrait consacrer un principe général, le surplus relevant des réglementations nationales et de la coopération internationale[48.]. Mais un sondé considère qu'il n'est simplement pas désirable que la Convention tranche la question du droit applicable à la protection des données[49.].

---

[36] Avis EFAMRO-ESOMAR.
[37] Avis de l'AEDH ; avis de l'AFAPDP et l'OIF ; avis CNIL ; avis Spyros Tsovilis ; avis Direcção-General da Politica de Justica .
[38] Avis CNIL.
[39] Voy. par exemple avis UK Ministry of Justice .
[40] Avis commun de l'AFME et de la BBA.
[41] Avis Bulgaria-Commission pour la protection des données personnelles ; Avis Cyprus-Data Protection Commissioner; Avis Czech Republic – The office for personal data protection; avis Lithuania-State data protection inspectorate ; avis Ile Maurice-Commissariat à la protection des données; avis mydex (point 24) ; avis Ukraine-Data protection authority.
[42] Avis EPA; Avis German Insurance Association.
[43] Avis CNIL ; avis Cyberspace Law and Policy Centre ; avis EBF ; avis CLSR-IAITL-ILAWS ; avis Privacy International. Le T-PD devrait ainsi étudier la question, avis Direcção-General da Politica de Justica .
[44] Dans l'avis Albania-Data Protection Commissioner, il est souligné qu'il faudrait prévoir dans la Convention une règle permettant aux Etats d'établir des règles spécifiques en la matière.
[45] Avis CNIL.
[46] Avis CLSR-IAITL-ILAWS.
[47] U.S. Federal Trade Commission.
[48] Ukraine-Ministry of justice.
[49] Avis Italy-Garante per la protezione dei dati personali.

178. Quoi qu'il en soit, différents avis offrent des pistes de réflexion quant à la détermination du droit applicable à la protection des données.

179. Au niveau des **critères de rattachement**, différentes propositions se dégagent des avis. Par exemple, chaque Etat garantissant une protection équivalente – on se situerait, par exemple, au sein de l'Union européenne –, une entreprise agissant dans plusieurs de ces Etats ne serait tenue au respect que d'une seule réglementation : celle de son lieu de principal établissement[50]. Selon certains répondants, les règles de chaque Etat devraient être considérées équivalentes[51]. On observe de manière générale que certains répondants souhaitent le jeu d'un « country of origin principle »[52.]

180. D'autres nuances sont proposées quant aux critères de rattachement. Certains proposent que soit pris en compte, à titre principal, le critère du lieu d'établissement du responsable de traitement et qu'à titre secondaire, ce soit celui du lieu vers lequel le responsable de traitement dirige son activité de façon spécifique[53]. Le critère de la direction des activités serait un critère à prendre en compte en particulier lorsque le responsable de traitement est établi en dehors du territoire de l'UE[54]. Il est parfois suggéré que le droit du pays où la plus importante part des opérations de traitement a lieu soit applicable ou, si cela ne peut être déterminé, le droit du pays de localisation du responsable de traitement[55].

181. Dans un autre sens, des répondants vont jusqu'à considérer que lorsque plusieurs juridictions sont concernées, « les personnes concernées devraient être en droit de se réclamer de la législation la plus protectrice en cas de problème »[56]. Ou encore, que le droit applicable à la protection des données devrait être celui de la « victime »[57] – personne concernée. Le cas échéant, cette règle vaudrait en tant que principe et des exceptions pourraient être aménagées[58].

182. Quels que soit les critères finalement retenus, des **considérations à prendre en compte** dans leur définition sont évoquées par les sondés. Ainsi, s'il s'agit de veiller à réduire le risque de « *forum shopping* »[59], il faudrait aussi limiter les « *compliance burdens* » pesant sur les entreprises[60]. Dans le même sens, une simplification des règles est demandée quant aux entreprises appartenant à un même groupe international ayant des activités transfrontières[61], notamment en clarifiant les responsabilités au sein de tels groupes.

183. Certains jugent que toute évolution des règles en cause devrait impliquer une amélioration de la libre circulation des données à caractère personnel[62]. La modification des règles de droit international privé ne doit pas entraîner un

[50] Avis EPA.
[51] Avis APEP.
[52] Avis FEDMA ; avis Techamerica Europe .
[53] Avis CNIL
[54] Avis APEP
[55] Avis EPA
[56] Avis de l'AEDH
[57] Avis Sénégal-Commission à la protection des données.
[58] L'avis Direcção-General da Politica de Justica semblerait aller dans le même sens, recommandant l'applicabilité de la loi de la personne concernée, en ce qu'il renvoie à la « loi nationale ». Il souligne toutefois que des exceptions devront certainement être adoptées, en particulier quant au contexte de l'Union européenne.
[59] Avis CEA.
[60] Avis CEA ; avis EMOTA ; avis ENPA-FAEP; FEDMA.
[61] Avis Data Industry Platform ; avis GDD.
[62] Avis commun de l'AFME et de la BBA ; avis Data Industry Platform ; avis EMOTA ; avis FEDMA.

désavantage compétitif pour le marché intérieur (UE)[63]. Il ne faudrait pas non plus introduire une « *extra jurisdictional reach* »[64]. Pour éviter ce dernier travers, il serait recommandé de tenir compte de la volonté des individus de recourir aux services de prestataires totalement en dehors de l'Espace Economique Européen (EEE-EEA), et privilégier la prise de décision correctement informée[65].

184. Dans un autre ordre d'idées, les règles déterminant le droit applicable ne devraient pas permettre, aux demandeurs en justice contre des entreprises de médias, de choisir un forum où les règles de protection sont plus strictes que celles de l'Etat d'établissement de ces entreprises, ce qui entraînerait un risque pour la liberté d'expression[66].

185. Une disposition de la Convention sur le droit applicable ne devrait pas contrarier la protection nationale offerte aux consommateurs[67].

186. Il faudrait encore prendre en compte le fait que la modification des règles déterminant le droit applicable n'ont pas seulement une incidence sur les relations « B2C » mais également sur les relations entre entreprises et autorités gouvernementales, dont les « *law enforcement authorities* »[68].

187. Enfin, si la question du droit applicable est souvent traitée par les avis rendus, certains évoquent les critères de compétence et la nécessité qu'ils soient pragmatiques – le cas échéant, une distinction pourrait aussi être opérée entre la compétence civile et la compétence pénale ; il conviendra que le T-PD se penche sur cette question[69].

Autorités de protection des données

25. Comment garantir leur indépendance et assurer une coopération internationale entre les autorités nationales ?

188. Une meilleure coopération est demandée[70]. Des répondants relèvent que la coopération entre autorités de protection des données devrait sans doute faire l'objet de mesures complémentaires inscrites dans la Convention[71] – d'autres ne sont pas du même avis, laissant le problème au droit national[72] –, de mécanismes internationaux facilitant la coopération transfrontière pour l'application des droits de la protection des données[73], mécanismes à définir – tels qu'un forum commun[74] ; le minimum d'exigences devrait en tout cas être prévu[75]. Il s'agirait alors de préciser et faciliter la coopération internationale – conditions de coopération, modalités des

[63] Avis APEP.
[64] Avis commun de l'AFME et de la BBA.
[65] Avis commun de l'AFME et de la BBA.
[66] Avis ENPA-FAEP.
[67] Avis CIPPIC.
[68] Avis Techamerica Europe .
[69] Avis Direcção-General da Politica de Justica.
[70] Avis commun de l'AFME et de la BBA.
[71] Avis AEDH
[72] Avis CLSR-IAITL-ILAWS ; avis Privacy International ; avis Ukraine-Ministry of justice.
[73] Avis EBF.
[74] Avis Italy-Garante per la protezione dei dati personali.
[75] Avis Lithuania-State data protection inspectorate.

actions communes –, mais de ne pas l'imposer[76]. Certains estiment au contraire que la coopération doit être imposée pour les problèmes globaux[77].

189. Il est aussi proposé que les autorités puissent conduire des investigations conjointes sur le territoire de plusieurs Etats membres – plaintes internationales, contrôles transfrontières – [78], sans pour autant que cela ne mette en péril leur financement[79]. Dans ce cadre, il importe de clarifier les pouvoirs d'actions des autorités à l'étranger[80]. D'autres notent qu'il devrait être travaillé à une meilleure reconnaissance entre autorités de protection des données des mesures prises par elles – y compris les notifications[81]. Un répondant va jusqu'à proposer la création d'une autorité supranationale[82].

190. Il a enfin été relevé que l'article 13, § 3, b), de la Convention était un obstacle à la coopération internationale entre autorités en ce qu'il empêchait le transfert des données à caractère personnel impliquées dans le traitement litigieux alors que cela est nécessaire en vue de la résolution des différends[83].

191. Concernant l'indépendance de ces autorités de contrôle, la Direcçao Geral da Politica de Justiça portugaise propose les critères suivants : Il faut des garanties que l'autorité de protection des données n'est pas assujettie à des instructions ou à des conditions susceptibles de gêner sa capacité de décision indépendante, c'est-à-dire sans une quelconque interférence d'aucune entité publique ou privée, et qu'elle dispose, par le biais du budget public, des moyens nécessaires à son fonctionnement.

26. Leur rôle et leurs tâches devraient-ils être spécifiés ?

192. Oui. L'AEDH relève que le protocole additionnel est peu explicite sur les missions et les pouvoirs des autorités de contrôle. Les exemples contenus dans le rapport explicatif mériteraient tous d'être codifiés dans le texte même du protocole. Le CLPC invite à transférer la disposition dans la Convention elle-même.

193. Pour le ICUK, une clarification serait la bienvenue dans un paysage où les autorités nationales existantes présentent un patchwork bigarré. Leur rôle éducatif devrait en tout les cas être maintenu. La CNIL estime qu'il conviendrait de renforcer le pouvoir de contrôle *a posteriori* de ces autorités. La Commission bulgare demande qu'on veille à ne pas surcharger de manière infondée ces autorités. Le CLPC insiste sur une tâche en particulier : l'obligation de rendre des comptes notamment au public sur les obligations de traiter les plaintes. Tandis que pour le Garante il serait important d'apporter des précisions sur les mécanismes de coopération entre autorités, peut-être en envisageant des mécanismes d'interaction spécifiques ou des forums communs.

194. En outre, aux yeux de l'EPA et de l'APEP, leurs décisions devraient être reconnues mutuellement par les autres Etats Parties, ce serait appréciable, notamment concernant les BCR. Le CIPPIC invite à réfléchir à rendre les décisions des autorités

[76] Avis CNIL.
[77] Avis APEP.
[78] Avis Bulgaria-Commission pour la protection des données personnelles ; Avis CNIL.
[79] Avis Bulgaria-Commission pour la protection des données personnelles.
[80] Avis CNIL.
[81] Avis Techamerica Europe.
[82] Avis Sénégal-Commission à la protection des données.
[83] Avis United Kingdom-Information commissioner's office.

de contrôle juridiquement liantes par le biais du concept de *common law* de *stare decisis*.

Flux transfrontières de données

27. La Convention 108 avait pour but de concilier la protection effective des données et la libre circulation de l'information sans considération de frontières. Ces principes ont été développés plus avant dans un protocole additionnel (STCE 181, 2001). En principe, un niveau de protection adéquat doit être assuré.

28. Doit-on entièrement réexaminer la notion de « flux transfrontières de données » à l'heure d'Internet, où les données circulent instantanément à travers les frontières ? Serait-il utile de fixer des règles minimales internationalement reconnues pour garantir le respect de la vie privée sans considération des frontières ? Quel pourrait en être le contenu ?

29. Doit-il y avoir des règles différentes pour le secteur public et le secteur privé ? S'agissant notamment du secteur privé, doit-on avoir davantage recours à des règles d'entreprise contraignantes, éventuellement associées à un système de responsabilisation du destinataire final pour garantir le respect de ces règles ?

195. Les questions relatives aux FTD sont à lire en parallèle avec la problématique du droit applicable à la protection des données. Un répondant émet un avertissement : dans un monde en réseau, il y a des limites à la mesure dans laquelle les flux de données peuvent ou doivent être contrôlés[84].

196. Différents intervenants soulignent que l'approche actuelle du régime des flux transfrontières de données n'est pas adaptée à la situation actuelle du contexte technologique[85] ; les individus impliqués dans le monde virtuel font passer leurs données d'une juridiction à l'autre via de simples clicks, le cas échéant à destination de pays tiers à l'UE ne garantissant pas de protection adéquate[86]. L'approche actuelle ne fonctionne pas de manière efficace, étant pesante pour ceux agissant de manière bénigne, et inefficace vis-à-vis de ceux qui sont plus malicieux[87]. La problématique des FTD devrait être traitée de manière plus réaliste[88]. A tout le moins, il devrait être spécifié, dans le contexte d'Internet, quand ont lieu de tels transferts[89] ; le concept de FTD doit être clarifié voire reconsidéré[90]. A l'occasion de la revendication d'un système plus praticable, les travaux de l'APEC ont été évoqués[91].

[84] Avis CLSR-IAITL-ILAWS.
[85] Avis commun de l'AFME et de la BBA ; Avis Czech Republic – The office for personal data protection .
[86] Avis Techamerica Europe .
[87] Avis CLSR-IAITL-ILAWS.
[88] Avis United Kingdom-Information commissioner's office.
[89] Avis Albania-Data Protection Commissioner ; avis Bulgaria-Commission pour la protection des données personnelles.
[90] Avis EBF ; Avis Italy-Garante per la protezione dei dati personali.
[91] Avis U.S. Federal Trade Commission.

197. Différents répondants estiment que « l'approche de principe » « ne devrait pas être modifiée » en ce qu'une protection adéquate est exigée[92]. Dans le même sens de l'exigence d'une protection adéquate, il a été souligné que les dispositions du protocole additionnel devraient être intégrées à la Convention[93], le cas échéant en précisant les règles[94]. Au contraire, certains demandent un nouvel instrument légal, séparé de la Convention, et contenant les règles détaillées nécessaires[95]. D'autres encore notent que le caractère de la Convention est général et qu'il appartiendrait plutôt aux Etats membres de traiter cette question compliquée[96], alors que les différences nationales exacerbent les difficultés pratiques actuelles[97].

198. La définition de l'adéquation intéresse les répondants. Des répondants considèrent qu'il faudrait établir une liste des garanties minimales définissant le standard du niveau adéquat de protection[98], le cas échéant en s'inspirant de ce qui se fait au niveau de l'Union européenne[99]. Selon certains, la Convention 108 devrait expressément reconnaître les décisions d'adéquation de la Commission européenne prises sur le pied de l'article 26 de la directive 95/46[100]. D'autres critiquent toutefois ce qui se fait au niveau européen en soulignant que ce qu'exige la Commission relève parfois plus de l'équivalence que de l'adéquation[101] ; la Convention devrait réaffirmer que ce n'est que l'adéquation qui est exigée[102]. Aussi, le processus pourrait être plus rapide et plus simple[103]. La Convention pourrait rendre le processus d'évaluation plus transparent et pourrait dans ce cadre être à la source du développement de standards largement reconnus[104].

199. Plus spécifiquement, il est suggéré que l'appréciation du caractère adéquat puisse être effectuée sur la base de larges secteurs de traitement de données – secteur financier, sous-traitance informatique, PNR, etc. – [105] ; par ex., un secteur serait réputé garantir une protection adéquate, même si le pays de son établissement n'offre pas des garanties adéquates de protection[106]. Ainsi, l'adéquation ne devrait pas être une analyse générale du droit de l'Etat tiers concerné, mais elle devrait être plus liée aux circonstances particulières du cas d'espèce, en particulier au responsable de traitement – ou sous-traitant – situé dans l'Etat tiers, le droit de cet Etat n'étant qu'un élément d'analyse parmi d'autres[107]. Certains lient aussi directement le principe de la protection adéquate au principe d' « *accountability* »[108].

---

[92] Avis de l'AEDH. Favorable à l'exigence du standard de la protection adéquate, voy. encore avis UK Ministry of Justice.
[93] Avis Cyberspace Law and Policy Centre ; avis CLSR-IAITL-ILAWS ; avis Privacy International ; avis Direcção-General da Politica de Justica.
[94] Avis CLSR-IAITL-ILAWS.
[95] Avis Cyprus-Data Protection Commissioner.
[96] Avis FEDMA.
[97] Avis CLSR-IAITL-ILAWS.
[98] Avis Albania-Data Protection Commissioner ; avis Bulgaria-Commission pour la protection des données personnelles.
[99] Avis Albania-Data Protection Commissioner .
[100] Avis APEP.
[101] Avis CLSR-IAITL-ILAWS.
[102] Avis United Kingdom-Information commissioner's office.
[103] Avis United Kingdom-Information commissioner's office.
[104] Avis CLSR-IAITL-ILAWS.
[105] Avis Albania-Data Protection Commissioner; avis APEP.
[106] Avis United Kingdom-Information commissioner's office.
[107] Avis United Kingdom-Information commissioner's office. Constate également que la situation du receveur des données n'est pas prise en compte l'avis U.S. Federal Trade Commission ; avis UK Ministry of Justice, faisant référence à la Déclaration de Madrid comme point de départ de la réflexion.
[108] Avis Techamerica Europe ; avis United Kingdom-Information commissioner's office.

200. Dans le contexte de l'Union européenne, lorsqu'un pays tiers ne garantit pas une protection adéquate, différents outils peuvent néanmoins permettre les FTD. A cet égard, certains demandent qu'il y ait, dans le contexte de l'Union européenne, une meilleure reconnaissance des « *Binding Corporate Rules* » [BCR] ou « *Model Contractual Clauses* » [MCC], de telle sorte que les transferts de données ayant lieu au sein d'un même groupe international d'entreprises soumis aux mêmes règles strictes ne doivent pas faire l'objet d'une autorisation spécifique des autorités de protection des données[109] ; les règles devraient être simplifiées[110]. Le régime d'autorisation est problématique quant au temps et aux frais qu'il nécessite[111], il conviendrait de procéder à un allègement des formalités en cas de recours aux MCC ou aux BCR approuvées par les autorités[112]. Plus de flexibilité est d'ailleurs demandée quant aux clauses contractuelles types qui, à l'heure actuelle dans l'Union européenne, ne reflètent par exemple pas la réalité du « *Cloud Computing* », rendant le modèle inapproprié[113]. Il serait également opportun de promouvoir des codes de conduite sur les FTD qui seraient acceptés par toutes les autorités de protection des données pertinentes[114].

201. Des répondants considèrent que des règles internationales minimales devraient être établies quant aux FTD[115]. Ce qui est l'objectif de la résolution de Madrid qu'il conviendrait d'incorporer dans un texte liant[116]. Mais dans toutes les hypothèses où de telles règles minimales seraient souhaitables, il conviendra de garder en vue le potentiel risque d'une « *race to the bottom* »[117] ; des répondants estiment qu'une telle course serait la conséquence nécessaire d'une tentative d'établir des règles minimales globales, détruisant la protection de la vie privée dans un contexte transfrontière, et rendant donc ce minimum non souhaitable[118]. D'autres rappellent qu'avant de penser aux standards minimums globaux, il faudrait établir le cadre procédural de leur élaboration, mettant en jeu toutes les régions et tous les intéressés[119].

202. Enfin, dans un autre registre, le « *Data Protection Officer* » [DPO] pourrait avoir un rôle en matière de FTD, et un DPO européen pourrait être nommé pour un groupe de sociétés présent dans différents pays de l'Union européenne[120].

[109] Avis commun de l'AFME et de la BBA.
[110] Avis Data Industry Platform; avis EMOTA.
[111] Avis German Insurance Association.
[112] Avis AFCDP (p. 4).
[113] Avis commun de l'AFME et de la BBA.
[114] Avis CEA.
[115] Avis CEA ; Avis Cyprus-Data Protection Commissioner; Avis EPA ; Avis German Insurance Association; avis AFCDP.
[116] Avis APEP.
[117] Avis CIPPIC.
[118] Avis Cyberspace Law and Policy Centre; avis CLSR-IAITL-ILAWS ; avis Privacy International .
[119] Avis U.S. Federal Trade Commission.
[120] Avis AFCDP.

Rôle du comité consultatif

30. La Convention 108 a créé un comité chargé de faciliter son application et, le cas échéant, de l'améliorer. Doit-on renforcer le rôle jusqu'ici principalement consultatif du comité ? Si oui, quelles fonctions faut-il développer plus avant : l'activité normative, le règlement des litiges, le suivi ?

203. La plupart de ceux qui ont répondu à cette question sont favorables au renforcement du rôle du Comité consultatif, tandis que quelques répondants estiment que le rôle doit demeurer inchangé.

204. Le Comité devrait évoluer vers une véritable autorité de protection des données, chargée en matière de suivi d'identifier très en amont les innovations et de les accompagner de recommandations, et en matière de litige, de pouvoir être saisie lorsque des parties prenantes sont confrontées à un problème transfrontalier (AEDH). Le Commissaire à la protection des données de l'Ile Maurice souligne qu'en matière de litiges, il conviendrait que les autorités nationales mais aussi les individus puissent saisir ce Comité transformé en autorité contraignante. Un rôle de suivi renforcé permettrait de vérifier la manière dont la Convention est mise en œuvre au niveau national et de disposer de moyens d'action en cas de mauvaise mise en œuvre (CNIL). Un renforcement du rôle ne devrait porter que sur des fonctions de surveillance (CEA Insurers of Europe), ou sur ces fonctions mais également sur l'édiction de standards (Commissaire à la protection des données de Chypre ; consortium CLSR-IAITL-ILAWS), voire que sur l'édiction de standards (European Privacy Association). Un rôle de coordination des pratiques, expériences et suggestions des autorités nationales de protection des données devrait être assumé par ce Comité, de même qu'un rôle de suivi au niveau de la coopération internationale (Office for National Data Protection de la République tchèque ; State Data Protection Inspectorate de Lituanie). Enfin, on devrait leur reconnaître un rôle d'élaboration législative.

205. Il faut toutefois veiller à ce que cela n'induise pas des charges supplémentaires pour les Etats parties et pour les autorités nationales. Il faudra être attentif à éviter toute duplication avec les autres organismes supranationaux existants et éviter d'adopter des standards contradictoires (ICUK). Pour la Data Industry Platform, le risque de duplication est avéré et ils sont opposés à l'idée d'ajouter une couche supplémentaire aux institutions déjà existantes. Pour eux, l'élaboration de standards, la résolution de litiges et les fonctions de suivi sont des matières dans lesquelles l'autorégulation est la réponse la plus adéquate.

206. L'autorité de protection des données chypriote et le Garante italien relèvent tous deux que tout renforcement de rôle du Comité sera dépendant d'une mise à disposition de moyens humains et financiers. Pour le Garante, il conviendrait donc d'adopter des dispositions visant à garantir la mise à disposition de telles ressources.

207. La CNIL fait une suggestion à propos de la composition de ce Comité. Etant donné le rôle « absolument essentiel » de ce comité dans l'architecture du travail du Conseil de l'Europe, la CNIL estime qu'il serait extrêmement souhaitable de revoir la composition de cet organe. Etant donné que ce sont les autorités de protection des données qui sont les premières en charge d'appliquer la Convention 108, que ces autorités bénéficient de l'expérience et de l'expertise pratique, à l'inverse du gouvernement, ce devrait être elles qui désignent un représentant pour composer le

Comité et non les gouvernements. Les représentants de gouvernements sont eux les seuls présents au Comité directeur de coopération juridique qui intervient dans le processus d'élaboration des textes.

208. La FTC américaine suggère que la révision de la Convention soit l'occasion de réfléchir à l'apport et au soutien que le Comité pourrait rechercher auprès de l'industrie et d'autres acteurs clés. Le rôle et le travail de l'ENISA Permanent Stakeholder Group pourrait peut-être être pris comme exemple de comment obtenir un apport et faciliter le dialogue avec l'industrie sur la Convention, étant donné le rôle important que ce groupe joue dans le cadre juridique de la protection des données de l'UE et ailleurs dans le monde.