Strasbourg, 19 septembre 2013 T-PD-BUR(2013)3rev2

BUREAU DU COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL (T-PD-BUR)

Projet de rapport explicatif de la version modernisée de la Convention 108

(sur la base des propositions adoptées par la 29e réunion plénière du T-PD)

DG I – Droits de l'homme et Etat de droit

I. INTRODUCTION

Historique

Le Comité consultatif (T-PD) de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après la « Convention 108 ») a décidé lors de sa 25e réunion plénière (2-4 septembre 2009) de fixer comme priorité numéro un de son « programme de travail pour 2009 et les années à venir » la préparation d'amendements à la Convention 108.

Le T-PD a en particulier identifié plusieurs angles d'approche potentiels pour ce travail sur la convention, comme les développements technologiques, les décisions individuelles automatisées, les informations à fournir à la personne concernée, et l'évaluation de la mise en œuvre de la Convention 108 et de son protocole additionnel par les Etats contractants.

Les priorités proposées ont été officiellement approuvées par le Comité des Ministres en mars 2010. Les Délégués des Ministres (1079e réunion, 10 mars 2010) ont salué l'adoption du programme de travail du T-PD et ont encouragé le T-PD à commencer à travailler à la modernisation de la Convention 108.

Les ministres participant à la 30e Conférence du Conseil de l'Europe des ministres de la Justice (Istanbul, Turquie, 24-26 novembre 2010) ont en outre exprimé leur soutien à la modernisation de la Convention 108 dans leur Résolution n° 3 sur la protection des données et la vie privée au troisième millénaire.

L'Assemblée parlementaire du Conseil de l'Europe a également accueilli avec satisfaction cet exercice de modernisation dans sa Résolution 1843(2011) sur la protection de la vie privée et des données à caractère personnel sur l'internet et les médias en ligne.

Le T-PD a commencé les travaux en chargeant des experts d'établir un rapport[1], en vue d'identifier les domaines dans lesquels une modernisation de la Convention 108 serait nécessaire afin de faire face aux nouveaux défis posés par les technologies de l'information et de la communication.

Un deuxième rapport[2] a été préparé afin d'aborder un autre aspect crucial de la modernisation : l'évaluation de la mise en œuvre de la Convention 108 par les Parties contractantes.

En s'appuyant sur le premier rapport, le T-PD a élaboré une liste de questions à examiner dans le contexte de la modernisation et un document de consultation[3] comportant 30 questions.

---

[1] Rapport sur les lacunes de la Convention nº 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (T-PD-BUR(2010)09), établi par Cécile de Terwangne, Jean-Marc Dinant, Jean-Philippe Moiny, Yves Poullet et Jean-Marc Van Gyseghem (CRIDS, université de Namur).

[2] Rapport sur les modalités et les mécanismes d'évaluation de la mise en œuvre de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE nº 108) et son protocole additionnel (T-PD-BUR(2010)13Rev), établi par Marie Georges.

[3] http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf.

Ces 30 questions ont été soumises à une consultation publique afin de recueillir des réactions et commentaires à l'occasion du 30e anniversaire de la Convention 108, le 28 janvier 2011 (5e édition de la journée de la protection des données). Cette consultation publique visait à permettre à toutes les parties concernées (particuliers, société civile, secteur privé, organismes de surveillance, autorités de contrôle) – dans le monde entier – de donner leur avis sur l'avenir de la Convention 108.

De nombreuses contributions ont été reçues de la part de répondants issus des secteurs public (autorités gouvernementales et autorités de protection des données) et privé (monde bancaire, des assurances, du commerce électronique, du marketing, de la diffusion audio-visuelle, de la recherche socio-économique, etc.), des milieux universitaires et des associations intéressées. Les réponses provenaient en outre de plusieurs continents et non pas de la seule Europe.

Il a fallu trois réunions du Bureau du T-PD en 2011 pour transformer ces informations denses et extrêmement riches[4] en propositions concrètes de modernisation[5] de la Convention 108. Ces propositions ont été examinées en première lecture par la 27e réunion plénière du T-PD (30 novembre-2 décembre 2011).

Dans le prolongement des discussions tenues lors de cette 27e réunion plénière et compte tenu des différents projets soumis pour commentaire, plusieurs versions[6] des propositions de modernisation ont été préparées par le Bureau du T-PD. Les projets successifs ont été soumis pour commentaire non seulement au T-PD, mais également à plusieurs comités du Conseil de l'Europe, ainsi qu'à des parties intéressées du secteur privé et de la société civile (notamment à l'occasion d'un échange de vues tenu le 2 mai 2012 dans le Bureau du Conseil de l'Europe à Bruxelles).

Lors de sa 28e séance plénière (19-22 juin 2012), le T-PD a examiné les propositions de modernisation de la Convention 108[7] en deuxième lecture et a chargé son Bureau de finaliser les propositions compte tenu de ces discussions et commentaires, en vue de leur examen lors de la 29e réunion plénière (27-30 novembre 2012).

Les propositions[8] et les commentaires écrits y afférents[9] ont été examinés en troisième lecture par la 29e séance plénière du T-PD et les propositions de modernisation[10] ont été adoptées pour transmission au Comité des Ministres, la finalisation des propositions devant être confiée à un comité intergouvernemental ad hoc.

Un projet de mandat du Comité ad hoc sur la protection des données personnelles (CAHDATA) a été préparé et examiné par le Bureau du T-PD[11] avant d'être transmis au Comité directeur Média et Société d'information (CDMSI), en vue de sa soumission au Comité des Ministres avec les propositions techniques du T-PD pour la modernisation de la Convention.

---

[4] Document T-PD-BUR(2011) 01 MOS rev 6.
[5] Document T-PD-BUR(2011)27 du 15 novembre 2011.
[6] Documents T-PD-BUR(2012)01Rev du 5 mars 2012 , T-PD-BUR(2012)01 du 18 janvier 2012.
[7] Documents T-PD-BUR(2012)01Rev2 du 27 avril 2012 et T-PD(2012)04 Rev.
[8] Document T-PD(2012)04Rev2.
[9] Documents T-PD(2012)11Mos et Addendum.
[10] Voir annexe III du rapport abrégé de la 29e réunion plénière du T-PD.
[11] 29e réunion du Bureau (5-7 février 2013).

Le 10 juillet 2013, lors de leur 1176e réunion, les Délégués des Ministres ont pris note des travaux menés par le T-PD concernant la modernisation de la Convention 108 et, en vue de la poursuite de ces travaux, ont approuvé le mandat du CAHDATA.

Modernisation : objectifs et principales caractéristiques

Chaque jour, de nouvelles menaces pèsent sur les droits de l'homme et les libertés fondamentales, notamment le droit à la vie privée. Il est devenu évident que la Convention 108 devait être modernisée afin de mieux relever les nouveaux défis en matière de protection de la vie privée découlant de l'utilisation grandissante des nouvelles technologies de l'information et des communications, de la mondialisation des processus et de l'ampleur croissante des flux de données à caractère personnel et de renforcer, en même temps, le mécanisme d'évaluation et de suivi de la convention.

Il ressort clairement des contributions reçues lors de la consultation publique de 2011 et des débats ultérieurs dans plusieurs forums qu'un large consensus se dégage sur les objectifs suivants : maintenir la nature générale et technologiquement neutre des dispositions de la convention (complétées par des textes sectoriels plus détaillés au moyen d'instruments juridiques non contraignants, notamment sous forme de recommandations du Comité des Ministres élaborées par le comité consultatif en consultation avec l'ensemble des parties prenantes) ; assurer la cohérence et la compatibilité de la convention avec d'autres cadres juridiques ; et réaffirmer le caractère ouvert de la convention, qui lui donne un potentiel unique d'instrument à vocation universelle.

La modernisation de la convention est d'une grande actualité. Etant donné la mondialisation croissante du traitement des données à caractère personnel (flux de données omniprésentes) et l'incertitude juridique qui en découle quant à la loi applicable, il est impérieux de veiller à ce qu'un socle commun de principes garantisse dans le plus grand nombre possible de pays du monde un niveau approprié de protection des personnes physiques à l'égard du traitement des données à caractère personnel.

La Convention 108 et les autres cadres internationaux

<u>Union européenne (EU)</u>

Le onzième considérant de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après la « Directive 95/46/CE ») est libellé comme suit :

« considérant que les principes de la protection des droits et des libertés des personnes, notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la convention, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ; »

Si la directive s'est fortement inspirée de la Convention 108 et visait à énoncer et amplifier les principes consacrés par cette dernière, elle n'est pas identique à la Convention 108. Par ailleurs, la cohérence et la compatibilité des deux cadres doivent être préservées à l'avenir. La nature générale des dispositions de la Convention 108 et les propositions de modernisation peuvent

certainement continuer d'être précisées et amplifiées par le cadre juridique proposé par l'Union européenne, les spécificités de chaque système étant dûment prises en considération.

L'Union européenne ne peut que continuer à soutenir une harmonisation accrue des lois relatives à la protection des données dans le monde entier, par le biais d'une adhésion plus large à la Convention 108.

Concernant les flux transfrontières de données, il faudrait à l'avenir assurer l'articulation entre les deux régimes afin de garantir leur compatibilité et leur complémentarité, ainsi que la nécessaire protection des personnes physiques dans le cadre de chaque régime. Le fait d'être Partie à la Convention 108 est un élément à prendre en considération lorsque l'Union européenne évalue d'adéquation du niveau de protection d'un Etat donné.

Organisation de coopération et de développement économiques (OCDE)

La rédaction de la Convention du Conseil de l'Europe et des Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel avait été placée sous le signe de la concertation. C'est dans un esprit de coopération renouvelé qu'ont été entrepris en parallèle les exercices de modernisation de la Convention et de révision des lignes directrices de 1980. Les deux organisations ont entretenu des liens étroits tant au niveau du Secrétariat qu'au niveau du Comité (chacune participant aux réunions en vertu de son statut d'observateur) en vue de maintenir la compatibilité entre les deux textes.

Forum de coopération économique de la région Asie-Pacifique (APEC)

Le cadre de l'APEC relatif à la protection de la vie privée et son récent dispositif d'encadrement du transfert de données personnelles au sein de ses pays membres (*Cross Border Privacy Rules system* – CBPR) ont été pris en considération, notamment dans le cadre de la réflexion engagée sur les modalités de la modernisation des dispositions relatives aux flux transfrontières de données. Ce processus a souligné la nécessité d'une compatibilité accrue entre les différents régimes.

PROJET DE RAPPORT EXPLICATIF

1. Le but du présent [protocole] est de moderniser les dispositions contenues dans la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) et son protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), et de renforcer leur application.

2. Depuis son ouverture à la signature, il y a 30 ans, la Convention 108 a constitué la clé de voûte du cadre juridique international de la protection des données dans plus de 40 pays européens. Elle a également influencé les politiques et les législations bien au-delà des rivages de l'Europe. Le Conseil de l'Europe modernise la Convention afin de répondre aux nouveaux enjeux en matière de protection des données découlant des évolutions technologiques, commerciales et sociales dans la société de l'information et de la communication ainsi que de la mondialisation croissante des échanges de données.

3. Les rapports explicatifs de la Convention 108 et de son protocole additionnel conservent toute leur pertinence : ils exposent le contexte historique et le processus normatif de ces deux instruments. Ces rapports doivent être lus en combinaison avec le présent document pour ces aspects particuliers.

4. Les travaux de modernisation ont été menés à bien en tenant dûment compte du cadre de l'Union européenne, des Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'Organisation de coopération et de développement économiques (OCDE), du cadre de l'APEC relatif à la protection de la vie privée, sans oublier d'autres travaux pertinents comme les « normes internationales sur la vie privée et la protection des données personnelles »[12] et les Lignes directrices concernant les fichiers informatisés de données personnelles (Nations Unies, 1990).

5. Le comité consultatif constitué en application de l'article 18 de la Convention (T-PD) a préparé les propositions de modernisation qui ont été adoptées lors de sa 29e réunion plénière (27-30 novembre 2012) et soumises au Comité des Ministres. [...]

6. Le texte du présent rapport explicatif ne constitue pas un instrument d'interprétation authentique du protocole, bien qu'il puisse guider et faciliter l'application des dispositions qui y sont contenues. Le présent protocole a été ouvert à la signature à ..., le ... .

Préambule

7. Le préambule réaffirme l'engagement des Etats signataires en faveur des droits de l'homme et des libertés fondamentales.

8. Mettre les individus en position de connaître, comprendre et donc contrôler le traitement de leurs données à caractère personnel est un objectif majeur de la Convention. En conséquence, le préambule mentionne expressément le droit de chacun de contrôler ses propres données, qui découle du droit à la protection de la vie privée, ainsi que de la dignité de la personne. La dignité

[12] Une initiative saluée par la 31e Conférence internationale des commissaires à la protection des données et de la vie privée, tenue à Madrid le 5 novembre 2009.

humaine implique la mise en place de garanties lors du traitement de données à caractère personnel afin que les individus ne soient pas traités comme de simples objets. Par conséquent, les décisions reposant uniquement sur un traitement automatisé des données ne sauraient être définitives si les personnes concernées n'ont pas le droit de faire valoir leur point de vue.

9. Compte tenu du rôle dans la société du droit à la protection des données à caractère personnel, le préambule souligne le principe selon lequel les intérêts, droits et libertés fondamentales des individus doivent, le cas échéant, être conciliés ainsi que la nécessité de prendre en considération le droit à la protection des données au même titre que la liberté d'expression et d'autres libertés et droits fondamentaux. Le droit à la « liberté d'expression » consacré par l'article 10 de la Convention européenne des droits de l'homme comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations. La Convention du Conseil de l'Europe sur l'accès aux documents publics[13] confirme en outre que l'exercice du droit à la protection des données, qui n'est pas absolu, ne saurait être utilisé d'une manière générale pour empêcher l'accès du public aux documents publics. Toutes les fois que l'exercice des droits à la liberté d'expression et d'accès aux documents publics est considéré comme étant soumis à des limitations en raison des droits à la protection de la vie privée et à la protection des données, il y a lieu de procéder à une mise en balance attentive de tous les intérêts en jeu dans chaque cas particulier, afin de ne pas indûment restreindre l'un de ces droits.

10. La Convention 108, à travers les principes qui y sont énoncés et les valeurs qu'elle contient, protège les individus et définit un cadre approprié pour le flux de l'information. Ceci est fondamental car les flux internationaux d'informations constituent une importante caractéristique sociétale qui permet en définitive l'exercice des libertés et droits fondamentaux. La protection des données ne doit certes pas être utilisée et employée intentionnellement comme un moyen d'ériger des barrières aux flux d'informations ou de restreindre les échanges d'informations, mais peut, dans certains cas, constituer une limitation légitime. Par ailleurs, les technologies innovantes devraient être utilisées comme un moyen de respecter les droits des individus. Cela aurait pour effet de conforter la confiance dans les innovations et les nouvelles technologies et, partant, de favoriser encore leur développement.

11. La coopération internationale entre les autorités de contrôle étant un élément clé d'une protection efficace des personnes physiques, la Convention vise à favoriser le renforcement de cette coopération, notamment en permettant aux Parties de se prêter mutuellement assistance et en fournissant le fondement juridique approprié pour établir un mécanisme formel d'échange d'informations à des fins de recherche et d'application.

Chapitre I – Dispositions générales

Article 1 – Objet et but

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

13. Les garanties énoncées dans la Convention s'étendent à toute personne physique relevant de la juridiction des Parties, indépendamment de sa nationalité ou de son lieu de résidence. Des clauses restreignant la protection des données aux ressortissants d'un Etat et aux étrangers résidant légalement sur son territoire sont donc incompatibles avec la Convention.

[13] STCE 205.

14. La portée de la protection dépend de la notion de « juridiction » des Parties afin de mieux résister à l'épreuve du temps et aux évolutions technologiques incessantes, ainsi qu'à l'évolution du concept juridique de juridiction de l'Etat en droit international, et de renforcer l'attachement à la protection des personnes physiques. La notion de « juridiction » s'entend au sens des compétences traditionnelles de l'Etat, c'est-à-dire ses compétences normatives, juridictionnelles et d'exécution.

15. Enfin, cet article met l'accent sur le sujet de la protection : les personnes physiques doivent être protégées lorsque leurs données à caractère personnel font l'objet d'un traitement. Ce droit a acquis une signification autonome au cours des trente dernières années. D'abord reconnu par la jurisprudence de la Cour européenne des droits de l'homme, qui a établi que « la protection des données à caractère personnel […] revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention[14] », il a ultérieurement été consacré comme un droit fondamental par l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Le droit à la protection des données à caractère personnel n'est pas un droit isolé mais un droit « habilitant » dans la mesure où il est essentiel d'en jouir pour exercer d'autres droits – comme le droit au respect de la vie privée – et libertés fondamentales.

Article 2 – Définitions

16. Les définitions figurant dans la présente Convention sont conçues pour s'appliquer uniformément à différents termes traduisant certains concepts fondamentaux dans les législations nationales.

Lettre a – « Données à caractère personnel »

17. « Personne identifiable » s'entend d'une personne qui peut être identifiée de façon raisonnablement aisée. Une personne physique n'est pas considérée comme « identifiable » si son identification nécessite des délais, des activités ou des moyens déraisonnables pour le responsable de traitement ou pour toute autre personne auprès de qui le responsable du traitement pourrait raisonnablement et légalement obtenir l'identification ou des moyens d'identification. La détermination de ce qui constitue des « délais, activités ou moyens déraisonnables » devrait être effectuée au cas par cas, en tenant compte de critères tels que le coût, les bénéfices d'une telle identification pour le responsable de traitement, etc.

18. Par « identifiable », on n'entend pas seulement faire référence à l'identité civile ou juridique en tant que telle de la personne, mais également à tout élément susceptible d'« individualiser » ou distinguer (et permettant ainsi de traiter différemment) une personne parmi d'autres, comme un numéro identifiant, des données de localisation, une adresse IP. Ces éléments permettent l'identification en renvoyant à une personne donnée ou à un point d'accès ou dispositif (ordinateur, téléphone portable, etc.).

19. Des données en apparence anonymes car non assorties de données d'identification évidentes peuvent néanmoins, dans certains cas, permettre d'identifier la personne à laquelle elles sont associées. C'est notamment le cas lorsque des caractéristiques physiques, physiologiques, génétiques, mentales, économiques, culturelles ou sociales (comme l'âge, le sexe, l'activité professionnelle, la géolocalisation, la situation de famille, etc.), seules ou en combinaison, permettent au responsable de traitement ou à tout acteur légitime ou illégitime (en

[14] Arrêt *M.S. c. Suède*, 1997, par. 41.

particulier lorsque les données ont été rendues publiquement disponibles) d'identifier la personne concernée. Dans de tels cas, les données ne sauraient être considérées comme anonymes et doivent être couvertes par les dispositions de la Convention.

20. Lorsque des donnés sont rendues anonymes, des mesures doivent être en place pour empêcher toute ré-identification des personnes. En particulier, tous les moyens techniques seront mis en œuvre pour garantir qu'elles demeureront anonymes. L'anonymat des données devrait être réévalué avec le temps. En effet, vu la rapidité des évolutions technologiques, toute chose qui pourrait à un moment donné être considérée comme « déraisonnable » pourrait, après un certain temps, être considérablement facilitée par la technologie et permettre une identification relativement aisée.

Lettre b [/c] – « Traitement de données »

21. L'expression « traitement de données » recouvre une notion très générale, susceptible d'une interprétation flexible. Partant de la collecte ou création de données à caractère personnel, elle couvre toutes les opérations automatisées, ainsi que les opérations partiellement ou entièrement « manuelles » effectuées sur des données organisées selon une structure qui permet de rechercher, combiner ou mettre en corrélation des données relatives aux personnes concernées par le traitement des données.

Lettre c [/d] – « Responsable de traitement »

22. « Responsable de traitement » désigne toute personne ou organe en charge du traitement en vertu d'une désignation officielle ou de son pouvoir de prise de décision à l'égard du traitement de données. Dans certains cas, il peut y avoir plusieurs responsables (en charge de différents aspects d'un traitement) ou coresponsables (conjointement responsables d'un traitement). Les critères ci-après sont pertinents pour savoir si la personne ou l'organe peut être qualifiée de responsable de traitement : les motifs justifiant le traitement ; les méthodes de traitement ; le choix des données à traiter ; enfin, qui est autorisé à y accéder. Le responsable du traitement demeure responsable des données traitées quelle que soit leur localisation. Les personnes qui se limitent à procéder aux opérations de traitement conformément aux instructions du responsable de traitement sont des sous-traitants.

23. Le pouvoir de prise de décision d'un responsable de traitement peut tenir au fait que le traitement des données à caractère personnel est sa principale activité (une agence de publicité qui traite des données personnelles pour produire des publicités ciblées par exemple), ou que le traitement constitue un support de son activité principale (création d'une base de données clients, traitement de données de clients afin de les défendre devant les tribunaux, plus généralement exécution d'un contrat, etc.). Dans toutes ces situations, un responsable de traitement conserve cette qualification lorsqu'il délègue à un tiers la responsabilité de mettre en œuvre des moyens ou éléments techniques aux fins du traitement. Dans ce cas, la société en question est un sous-traitant qui agit pour le compte du responsable de traitement, même si, *de facto*, elle prend des décisions concernant les modalités du traitement. Le responsable de traitement doit en tout cas veiller à ce que ces moyens ou éléments techniques ne soient pas contraires à l'objectif de protection des données, et à ce qu'ils soient appropriés eu égard aux finalités du traitement.

24. Dans la société de l'information, de plus en plus de responsables de traitement décident délibérément de recourir à des sous-traitants pour procéder aux opérations de traitement. Ceci

est à prendre en considération au sens où la définition des moyens de traitement apparaît aujourd'hui moins pertinente, eu égard à la qualification de responsable de traitement, que la définition de la finalité du traitement. Les responsables de traitement peuvent – et le font souvent – assumer consciemment la responsabilité de laisser aux prestataires la possibilité de définir les moyens techniques en jeu. Ces derniers ne sauraient être considérés comme des responsables de traitement pour cette seule raison. Cependant, ils peuvent indépendamment devenir responsables ou coresponsables (avec le responsable de traitement primitif) du traitement s'ils outrepassent délibérément les instructions données par le responsable primitif (par exemple s'ils modifient la finalité du traitement ou les règles régissant l'accès aux données à caractère personnel, ou s'ils décident d'ajouter des données à caractère personnel dans le cadre du traitement considéré, etc.). Il conviendra de répondre au cas par cas à cette question complexe de la qualification.

25. Toute opération de traitement doit être exécutée *conformément à la loi*, mais ne découle pas de la loi. Bien entendu, le traitement de certaines données à caractère personnel répond à une obligation légale (par exemple traitement de registres nationaux par une administration, collecte par un employeur des données de ses salariés à des fins de sécurité sociale ou fiscales, etc.). Dans ces situations, le pouvoir de prise de décision du responsable de traitement n'est pas lié à la décision de traiter des données à caractère personnel ; il est tenu de procéder au traitement conformément à la loi. Dans ces situations, la qualification de responsable de traitement peut être directement faite par la loi (par exemple par la loi qui prévoit spécifiquement l'obligation légale de procéder au traitement des données personnelles), mais elle doit parfois être faite au cas par cas (ainsi, lorsqu'un prestataire de services de la société de l'information décide de partager des informations avec des autorités publiques, par exemple pour les besoins d'une information judiciaire, ce prestataire de services est coresponsable du traitement en cause ; en revanche, lorsqu'il est tenu par la loi – par exemple en vertu d'une décision judiciaire – de fournir ce partage d'informations, cela ne devrait pas entraîner sa qualification de responsable de traitement – le responsable étant l'autorité publique qui demande les renseignements).

26. Aux termes de l'article 7 bis sur la transparence des traitements, le responsable – ou les coresponsables – du traitement fournit aux personnes concernées des informations sur son identité et sa résidence habituelle ou lieu d'établissement.

Lettre d [/e] – « Destinataire »

27. « Destinataire » désigne toute entité qui reçoit ou a accès à des données à caractère personnel. Suivant les circonstances, un responsable de traitement, un sous-traitant, la personne concernée ou un tiers peuvent être destinataires des données.

Lettre e [/f] – « Sous-traitant »

28. « Sous-traitant » désigne toute personne morale distincte qui agit pour le compte du responsable du traitement et accomplit les opérations de traitement conformément aux instructions du responsable du traitement et pour les besoins de ce dernier. Le salarié d'un responsable de traitement n'est pas un sous-traitant. Si un sous-traitant outrepasse les instructions du responsable du traitement et prend une décision relative au traitement (voir le paragraphe 23 / 24 sur le fait que prendre une décision quant aux moyens utilisés n'entraîne pas nécessairement la qualification de « responsable du traitement »), ce sous-traitant sera considéré comme un responsable de traitement aux fins de la Convention.

Article 3 – Champ d'application

29. Conformément au paragraphe 1, les Parties s'engagent à appliquer la Convention à tout traitement de données – dans le secteur public comme dans le secteur privé – soumis à la juridiction de la Partie concernée. Tout traitement de données effectué par un établissement public relève directement de la juridiction de la Partie concernée, étant donné qu'il est le produit de l'exercice de ses compétences. Les traitements de données effectués par des responsables de traitement du secteur privé relèvent de la juridiction d'une Partie lorsqu'ils présentent un lien suffisant avec le territoire de cette Partie, par exemple lorsque le responsable du traitement est établi sur le territoire de cette Partie ou lorsque des activités impliquant le traitement des données la concernant sont proposées à une personne dans ce territoire, étant donné que le principal critère de définition de la juridiction est toujours lié au territoire. La Convention est applicable lorsque les opérations de traitement des données relèvent entièrement de la juridiction de la Partie concernée. Les dispositions de l'article 12 s'appliquent en cas de flux transfrontières de données dans les secteurs public et privé.

30. Le paragraphe 1 bis exclut du champ de la Convention les traitements de données effectués pour l'exercice d'activités exclusivement personnelles ou domestiques. Cette exclusion vise à éviter l'imposition d'obligations déraisonnables à des traitements de données effectués par des personnes physiques dans leur sphère personnelle, non motivés par des activités professionnelles ou commerciales et correspondant exclusivement à des activités personnelles ou domestiques comme le stockage d'images sur un ordinateur, la création d'une liste comportant les coordonnées d'amis ou de membres de leur famille, la correspondance, etc.

31. Une activité sera « exclusivement personnelle ou domestique » suivant les circonstances. A titre d'exemple, lorsque des données à caractère personnel sont intentionnellement rendues accessibles à un grand nombre de personnes ou à des personnes manifestement étrangères à la sphère privée, l'exemption n'est pas applicable.

32. La Convention s'applique aux fournisseurs de produits et services, comme des logiciels ou applications, utilisés dans le cadre d'activités personnelles ou domestiques.

33. Lorsque le traitement porte sur des données relatives à des personnes physiques, chaque Partie peut prévoir dans son droit interne une extension de la protection des données relatives aux personnes morales afin de protéger leurs intérêts légitimes. La Convention s'applique à des personnes vivantes : elle n'a pas vocation à s'appliquer aux données des personnes décédées. Cependant, cela n'empêche pas les Parties d'étendre la protection aux personnes décédées (notamment pour répondre aux besoins croissants de protection de la réputation ou des intérêts de la personne décédée ou de ses héritiers).

Chapitre II – Principes de base pour la protection des données

Article 4 – Engagement des Parties

34. Comme cet article l'indique, la Convention oblige les Parties à incorporer des dispositions sur la protection des données dans leur droit interne. En effet, la Convention n'a pas été conçue pour être directement applicable et, par conséquent, les droits des individus ne peuvent en découler directement.

35. L'expression « droit interne » désigne, suivant le système juridique et constitutionnel du pays considéré, toutes les règles matérielles de nature contraignante, d'origine législative ou découlant de la jurisprudence qui répondent aux exigences qualitatives d'accessibilité et de

prévisibilité. Ceci implique que la loi doit être suffisamment claire pour permettre aux personnes physiques et autres entités de réguler leur propre comportement compte tenu des conséquences juridiques attendues de leurs actes, et que toute personne susceptible d'être concernée par cette loi doit y avoir accès. Cela couvre toutes les mesures applicables à un nombre illimité de cas et à un nombre indéterminé de personnes. Cela englobe les règles qui créent des obligations ou confèrent des droits aux personnes (physiques ou morales) ou qui régissent l'organisation, les pouvoirs et les responsabilités des autorités publiques, ou encore qui établissent des procédures. En particulier, cela englobe les Constitutions des Etats et tout acte écrit des autorités législatives (les lois au sens formel du terme). Cela couvre en outre non seulement toutes les mesures de réglementation (décrets, règlements, ordonnances et directives administratives) fondées sur ces lois, mais encore les conventions internationales applicables en droit interne, y compris le droit de l'Union européenne. S'agissant d'organisations internationales[15], l'expression « droit interne » s'entend du droit interne de ces organisations, qui dans certains cas peut avoir un effet direct, au niveau national, dans chacun des Etats membres. Cela englobe également toute règle de nature générale, de droit public ou privé (y compris le droit des contrats), ainsi que les décisions des tribunaux dans les pays de *common law* ou, dans tous les pays, une jurisprudence constante dans l'interprétation d'une loi écrite. Enfin, cela englobe tout acte d'un organisme professionnel exerçant en toute indépendance des pouvoirs délégués par le législateur, conformément à ses pouvoirs de réglementation.

36. De telles mesures contraignantes peuvent utilement être complétées par des mesures de réglementation volontaire dans le domaine de la protection des données, telles que des codes de bonne pratique ou des règles de conduite professionnelle. Toutefois ces mesures volontaires ne suffisent pas par elles-mêmes pour donner suite à la Convention.

37. L'efficacité de l'application des mesures prises pour donner effet aux dispositions de la Convention est d'une importance cruciale. Au-delà des dispositions législatives concrètes, le rôle de l'autorité (ou des autorités) de contrôle, ainsi que toute voie de recours mise à la disposition des personnes concernées par les données, devraient être pris en considération dans l'appréciation globale de l'efficacité de la mise en œuvre des dispositions de la Convention par chaque Partie.

38. Il est en outre énoncé au paragraphe 2 de l'article 4 que les mesures nécessaires pour donner effet à la Convention (à toutes les dispositions de la Convention) doivent être prises par les Parties concernées avant la ratification ou l'adhésion, c'est-à-dire avant que chaque Partie ne devienne juridiquement liée par la Convention. Cette disposition vise à permettre au comité conventionnel de vérifier a priori si toutes les « mesures nécessaires » ont été prises, pour veiller à ce que les Parties à la Convention respectent leurs engagements et assurent le degré de protection des données attendu dans leur droit interne. Le processus et les critères utilisés pour cette évaluation préadhésion doivent être clairement définis dans le règlement du comité conventionnel.

39. Chaque Partie s'engage au paragraphe 3 de l'article 4 à contribuer activement à cette évaluation du respect de ses engagements, en vue de permettre une évaluation régulière de l'application des principes de la Convention (ainsi que de son efficacité). La soumission régulière de rapports relatifs à l'application de leur législation en matière de protection des données pourrait être un élément possible de cette contribution active des Parties.

[15] Les organisations internationales sont définies comme des organisations intergouvernementales (Convention de Vienne sur le droit des traités entre Etats et organisations internationales ou entre organisations internationales, 1986).

40. Le comité conventionnel procèdera à l'évaluation de l'application en s'appuyant sur une procédure objective, équitable et transparente établie par le comité conventionnel et décrite en détail dans son règlement.

Article 5 – Légitimité des traitements de données et qualité des données

41. Le traitement de données doit être proportionné, c'est-à-dire approprié par rapport aux buts légitimes poursuivis, et nécessaire dans la mesure où ces buts ne peuvent être poursuivis par d'autres moyens appropriés moins attentatoires aux intérêts, droits et libertés des personnes concernées ou de la société. Le traitement de données ne peut induire une atteinte démesurée à ces intérêts, droits et libertés par rapport à ceux du responsable du traitement ou de la société. Le principe de proportionnalité doit être respecté à toutes les étapes du traitement.

42. Le paragraphe 2 prévoit que la légalité du traitement de données est subordonnée à l'une ou l'autre des deux conditions préalables essentielles ci-après : le consentement de la personne concernée ou une base légitime prévue par la loi. Les paragraphes 1 et 2 de l'article 5 sont cumulatifs et doivent être respectés afin de garantir la légitimité du traitement des données.

43. La personne concernée doit donner son consentement de manière spécifique, libre et éclairée et explicite / sans ambigüité. Elle doit être pleinement consciente des implications de sa décision et a été dûment informée à cette fin. Aucune influence ou pression, directe ou indirecte, ne peut être exercée sur la personne concernée. Des telles influences ou pressions peuvent, dans certains cas, être de nature économique. Ce peut être le cas lorsque, par exemple, la personne concernée doit donner son consentement au traitement des données, en l'absence d'autre alternative raisonnable et financièrement abordable, pour accéder à des services en ligne ou hors ligne largement reconnus comme essentiels dans la société contemporaine. Cependant, compte tenu du développement actuel de l'internet, il est admis que, par exemple, certains services en ligne ou des services additionnels puissent être subordonnés à l'acceptation d'un traitement de données personnelles limitées qui permettra une publicité ciblée raisonnable. Le consentement explicite / sans ambigüité est une manifestation de volonté : c'est la libre expression d'une action positive.

44. Le consentement, qui reflète la volonté de la personne, ne prévaut pas sur l'impératif de proportionnalité du traitement.

Néanmoins, le fait qu'il y ait eu un consentement valide de la personne concernée doit être dûment pris en considération dans le test de proportionnalité au stade de l'appréciation de la légitimité du traitement. Ce test est de la plus haute importance lorsque le consentement donné concerne des services essentiels. En effet, s'agissant de services essentiels, lorsque le consentement au traitement de données à caractère personnel est une condition de l'offre, si de nombreuses personnes seront enclines à donner leur consentement, d'autres pourront ne pas vouloir. Ces dernières subiront un préjudice – accès refusé – que la société pourrait vouloir éviter. Une façon d'éviter ce type de préjudice serait de considérer que compte tenu du traitement en cause, s'appuyer sur un consentement est disproportionné. Il s'agit dans une certaine mesure d'une question de nature publique à évaluer en fonction du degré de « paternalisme » de la Partie concernée. Le consentement peut également constituer un fondement général de la légitimité choisi par les responsables du traitement en raison de la certitude juridique qu'il est censé apporter. Toutefois, le test de proportionnalité sera toujours décisif dans l'évaluation de la légitimité du traitement.

45. La personne concernée est en droit de retirer son consentement à tout moment (ceci est à distinguer du droit distinct de s'opposer à un traitement). Cela n'aura pas d'incidence sur la légalité du traitement effectué avant le retrait du consentement.

46. Une finalité sera considérée comme légitime en fonction des circonstances. Le but est en effet de garantir dans chaque cas un juste équilibre entre tous les droits, libertés et intérêts en jeu : le droit à la protection des données à caractère personnel, d'une part, et la protection d'autres droits, d'autre part. Il faut par exemple ménager un juste équilibre entre les intérêts de la personne concernée et les intérêts du responsable du traitement ou de la société. Dans tous les cas, un traitement de données au service d'une intention frauduleuse ou malicieuse ne saurait reposer sur une finalité légitime.

47. La référence à une « finalité » spécifique indique qu'il ne sera pas permis de traiter des données pour des finalités non déterminées. Au contraire, la finalité précise du traitement doit être étayée par des données factuelles et être très soigneusement énoncée.

48. Lorsque la loi autorise un traitement de données pour une ou plusieurs finalités spécifiques, la présomption de légitimité du traitement est renforcée si des garanties supplémentaires sont fournies et si les principes de base de la Convention sont respectés. La loi doit elle-même respecter les principes de proportionnalité et de nécessaire détermination de la finalité.

49. La notion de « base légitime » prévue par la loi englobe le traitement de données nécessaire à l'exécution d'un contrat (ou de mesures précontractuelles), à la protection d'intérêts vitaux de la personne concernée, de l'intérêt général ou d'intérêts légitimes prépondérants.

50. Les conditions d'un traitement légitime sont énoncées au paragraphe 3 : les données sont traitées licitement et loyalement, et satisfont à des critères garantissant leur qualité. Les données doivent avoir été collectées pour des finalités explicites, déterminées et légitimes, et le traitement des données considérées doit être effectué pour ces finalité, ou du moins ne pas être incompatible avec ces finalités. La notion d'utilisation compatible doit être interprétée de façon restrictive de façon à ne pas nuire à la transparence, à la sécurité juridique, à la prédictibilité ou à l'équité du traitement de données. En particulier, les données à caractère personnel ne doivent pas faire l'objet d'un nouveau traitement que la personne concernée pourrait considérer comme inattendu, inapproprié ou contestable.

51. Le traitement ultérieur de données à caractère personnel pour une finalité statistique, historique ou de recherche scientifique est a priori jugé compatible pour autant que d'autres garanties soient prévues (comme, par exemple, des règles de secret professionnel, des dispositions régissant l'accès limité et la communication de données pour les finalités susmentionnées, notamment celles liées aux statistiques publiques et aux archives publiques, et d'autres mesures d'ordre technique et organisationnel visant à assurer la sécurité des données) et que le traitement des données pour une finalité statistique, historique ou de recherche scientifique ne constitue pas le fondement d'une décision à prendre à propos de la personne concernée, notamment d'une décision de nature administrative, judiciaire, fiscale ou autre. Il y a lieu de souligner que les opérations statistiques, par définition, excluent toute utilisation des renseignements obtenus pour des décisions ou mesures concernant une personne donnée.

52. Les données faisant l'objet d'un traitement doivent être adéquates, pertinentes, non excessives et limitées au minimum nécessaire par rapport aux finalités pour lesquelles elles sont traitées. Les données doivent en outre être exactes et, le cas échéant, mises à jour régulièrement.

53. La règle selon laquelle les données ne doivent pas être excessives par rapport aux finalités pour lesquelles elles sont traitées reflète le principe de proportionnalité : des données qui seraient pertinentes mais entraîneraient une atteinte démesurée aux libertés et droits fondamentaux en jeu ne doivent pas être traitées. Tel est le cas, par exemple, dans le secteur des assurances : il pourrait être utile de disposer du dossier médical complet d'une personne afin d'évaluer la pertinence d'un contrat d'assurance-vie, mais cela est manifestement excessif par rapport à la finalité du traitement. La règle selon laquelle les données ne doivent pas être excessives ne fait pas double emploi avec la règle selon laquelle les données sont limitées au minimum nécessaire.

54. L'exigence relative à la durée de la conservation des données à caractère personnel signifie que les données doivent être effacées une fois que la finalité pour laquelle elles ont été collectées a été atteinte ou qu'elles doivent être conservées sous une forme empêchant toute identification directe ou indirecte de la personne concernée.

Article 6 – Traitement de données sensibles

55. Le traitement de certaines catégories de données par des tiers, ou tout traitement de données fournissant des informations sensibles, peut conduire à empiéter sur les intérêts, droits et libertés et n'est autorisé que si une protection renforcée par des garanties appropriées, qui complètent les autres dispositions protectrices de la Convention, est prévue par la loi. C'est le cas, par exemple, lorsque cela touche à la sphère la plus intime de la personne concernée, ou lorsqu'il y a un risque potentiel de discrimination ou d'atteinte à la dignité d'une personne ou à son intégrité corporelle.

56. Afin d'éviter tout effet préjudiciable pour la personne concernée, le traitement de données sensibles pour des finalités légitimes doit être assorti de garanties appropriées (adaptées aux risques qui sont en jeu et aux intérêts, droits et libertés à protéger) appliquées seules ou de manière cumulative, par exemple : le consentement explicite de la personne concernée, une loi spécifique couvrant le but poursuivi et les modalités du traitement, le secret professionnel, une analyse de risque, une mesure d'ordre organisationnel ou technique.

57. Certaines catégories de données peuvent comporter un risque particulier pour les personnes concernées lorsqu'elles sont traitées, indépendamment du contexte du traitement. C'est notamment le cas des données génétiques qui peuvent être laissées par une personne et révéler des informations concernant la santé ou la filiation de l'intéressé, ainsi que de tiers. Les données génétiques sont toutes les données relatives aux caractéristiques génétiques d'une personne qui ont été héritées ou acquises à un stade précoce du développement prénatal. Elles résultent de l'analyse d'un échantillon biologique prélevé sur la personne concernée : analyse des chromosomes, de l'ADN et de l'ARN, ou analyse de tout autre élément permettant l'obtention d'informations du même ordre. Des risques analogues sont posés par le traitement de données concernant des infractions, des condamnations pénales (reposant sur le droit pénal et dans le cadre d'une procédure pénale) et les mesures de sécurité qui leur sont liées (impliquant une privation de liberté par exemple).

58. Le traitement de données biométriques – qui peuvent laisser des traces concernant une personne et sont uniques –, c'est-à-dire de données résultant d'une technique spécifique de traitement de données relatives aux caractéristiques physiques, biologiques ou physiologiques d'un individu et permettant l'identification ou l'authentification certaine de ce dernier, est

également considéré comme ayant un caractère sensible. Ceci n'implique pas que tous les traitements de « données biométriques » (comme les photos par exemple) doivent être considérés comme tels. Un traitement dit « sensible » s'entend plutôt d'un traitement qui conduirait à l'identification certaine d'une personne.

Certains traitements peuvent avoir un caractère sensible lorsque les données sont traitées en vue d'obtenir des informations spécifiques qu'elles vont révéler et qui, en l'occurrence, sont susceptible de nuire à la personne concernée. Ainsi, le traitement de noms de famille qui, dans certaines circonstances, ne présente aucun risque pour les individus, pourrait avoir un caractère sensible, par exemple si la finalité du traitement est de révéler l'origine ethnique ou les croyances religieuses des personnes sur la base de l'origine linguistique de leur nom. Le traitement de données en vue d'obtenir des informations relatives à la santé englobe le traitement d'informations concernant la santé passée, actuelle et future, physique ou mentale d'un individu, lequel peut être malade ou bien portant. Dans la plupart des cas, les données relatives à la santé sont à caractère sensible, mais il peut y avoir des situations où leur traitement ne risque pas de porter atteinte aux intérêts, droits et libertés de la personne concernée. Tel est notamment le cas des données vidéo. Leur traitement peut englober le traitement de données relatives à la santé des personnes filmées, par exemple le fait qu'elles portent des lunettes ou aient un bras cassé, mais il ne s'agit pas là de données qui seront prises en compte dans le cadre du traitement des données (sécurité) ; elles ne sauraient donc être qualifiées de données à caractère sensible. La même chose est vraie par exemple pour des données révélant l'origine ethnique de la personne concernée.

59. La liste des catégories de données sensibles contenue dans cet article n'a pas vocation à être exhaustive. Une Partie peut, conformément à l'article 11, incorporer dans son droit interne d'autres catégories de données sensibles dont le traitement sera autorisé ou restreint si ces données sont susceptibles de présenter un risque pour les individus.

60. Si des données sensibles font l'objet d'un traitement à finalité statistique, pour des motifs d'intérêt public (par exemple en vue de disposer de statistiques en matière d'égalité), elles ne doivent pas être conservées sous une forme identifiable plus longtemps que nécessaire, et des garanties appropriées doivent être en place (par exemple interdiction de publication ou de diffusion des données).

Article 7 – Sécurité des données

61. Des mesures de sécurité spécifiques, d'ordre technique et organisationnel, doivent être prises pour tout traitement en fonction de la nature des données à caractère personnel, du degré de vulnérabilité de l'architecture technique utilisée pour la réalisation du traitement, de la nécessité de restreindre l'accès aux données, des impératifs d'un enregistrement à long terme, etc. Les mesures de sécurité doivent être appropriées eu égard à la nature des données et aux finalités du traitement.

62. Les mesures de sécurité doivent être fondées sur l'état actuel des connaissances relatives aux méthodes et techniques de sécurité dans le domaine de l'informatique et leur coût doit être proportionné à la gravité et à la probabilité des risques potentiels. Elles doivent être revues et actualisées aussi souvent que nécessaire.

63. Si les mesures de sécurité visent à prévenir certains risques, le paragraphe 2 prévoit une obligation spécifique *ex post facto* au cas où une violation de données serait néanmoins intervenue et pourrait porter gravement atteinte aux libertés et aux droits fondamentaux de la

personne concernée. Un risque important d'atteinte à la vie privée, comme la révélation de données couvertes par le secret, d'atteinte à la réputation financière, de danger physique ou d'humiliation pourrait être jugé comme constitutif d'une atteinte « grave ».

64. En cas de violation de données à caractère personnel, le responsable de traitement est tenu de notifier l'incident aux autorités de contrôle. Il doit également notifier aux autorités de contrôle toute mesure prise ou proposée pour y remédier et pallier les conséquences potentielles.

65. Le fait d'avoir notifié les autorités de contrôle n'empêche pas le responsable du traitement de procéder à d'autres notifications complémentaires. Il devrait par exemple être encouragé à informer, le cas échéant, les personnes concernées et à leur fournir des renseignements adéquats et utiles leur indiquant notamment où s'adresser ainsi que les mesures à prendre pour atténuer les conséquences néfastes de la violation des données. La notification d'autres autorités compétentes, comme celles en charge de la sécurité des systèmes informatiques, pourrait également être exigée.

Article 7 bis – Transparence des traitements

66. Le responsable du traitement des données est tenu d'être transparent dans la conduite des opérations afin de garantir un traitement loyal et de permettre aux personnes concernées de comprendre et partant pleinement exercer leurs droits dans le contexte du traitement considéré.

67. Le responsable du traitement doit fournir un minimum d'informations aux personnes concernées lorsque leurs données sont collectées directement ou indirectement (par l'intermédiaire de tiers). Les exigences de transparence sont obligatoires, mais les informations sur le nom et l'adresse du responsable, la finalité des traitements effectués et les destinataires des données (qu'elles soient ou non évidentes) peuvent être fournies sous tout format approprié (par le biais d'un site web, d'outils technologiques sur des dispositifs personnels, etc.) pourvu que l'information soit bien présentée et facilement accessible pour les intéressés. L'information doit être lisible, compréhensible et adaptée aux personnes concernées. Tout autre renseignement nécessaire pour garantir un traitement loyal des données, comme la durée de conservation des données ou des informations sur les transferts de données vers un pays étranger (notamment si ce pays offre ou non un degré approprié de protection et les informations relatives aux mesures prises par le responsable du traitement pour garantir un niveau approprié de protection) doit également être fourni.

68. Le responsable du traitement n'est néanmoins pas tenu de fournir ces informations lorsque la personne concernée les a déjà reçues, dans le cas d'une collecte indirecte de données par le biais de tiers, lorsque cette éventualité est expressément prévue par la loi (la loi devrait être précise et suffisamment détaillée), ou lorsque cela lui est impossible parce que la personne concernée n'est pas directement identifiable ou que le responsable du traitement n'a aucun moyen de la contacter, ou bien lorsque cela implique des efforts disproportionnés. Une telle impossibilité peut aussi bien être juridique (dans le cadre d'une information judiciaire ou avec des avocats tenus à une obligation de confidentialité par exemple) que pratique (par exemple un responsable de traitement qui ne traite que des images ignore les noms et les coordonnées des personnes concernées).

69. Lorsqu'une telle impossibilité est d'ordre pratique ou lorsque la personne concernée a déjà été informée, le responsable du traitement des données doit néanmoins utiliser tous les moyens disponibles, raisonnables et économiquement abordables qui lui permettront d'informer les personnes concernées, d'une manière générale ou individuellement suivant les cas (par

exemple lorsque le responsable du traitement est mis en contact avec la personne concernée pour une raison quelconque, ou par le biais du site web du responsable du traitement, etc.).

Article 8 – droits des personnes concernées

70. Les dispositions énoncées dans cet article sont conçues pour permettre à toute personne concernée d'exercer et de défendre ses droits relatifs au traitement de données à caractère personnel la concernant.

71. Les principaux éléments de ces garanties sont notamment :
– le droit de toute personne de ne pas être soumise à une décision purement automatisée sans que son point de vue n'ait été pris en considération ;
– le droit de toute personne de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement ;
– le droit de toute personne d'être informée de l'existence d'un traitement de données la concernant et d'accéder aux données, ainsi que de connaître le contenu des informations ;
– le droit de toute personne d'être informée du raisonnement qui sous-tend le traitement de données et de le contester ;
– le droit de rectification ou d'effacement de données inexactes, erronées ou, d'une manière générale, de données dont le traitement est illicite ;
– le droit de disposer d'un recours si l'un quelconque des droits précédents n'est respecté ;
– l'assistance d'une autorité de contrôle.

Ces droits ne sont pas absolus et doivent être conciliés avec d'autres droits et intérêts légitimes. Ils peuvent, conformément à l'article 9, être limités pour autant que cela constitue une mesure nécessaire dans une société démocratique. Ainsi, le droit d'être informé du raisonnement qui sous-tend le traitement de données peut être restreint pour protéger les droits d'autrui, comme des secrets protégés par la loi (secrets commerciaux par exemple). En ce qui concerne le droit d'opposition, les opérations effectuées par le responsable du traitement sont considérées comme motivées par des raisons impérieuses et légitimes qui l'emportent sur les intérêts ou les droits et libertés de la personne concernée lorsque le traitement est prescrit par la loi (par exemple aux fins d'une enquête ou de poursuites dans le cadre d'infractions pénales) ou nécessaire à l'exécution d'un contrat, ou lorsque qu'un consentement valide a été donné pour le traitement considéré et n'a pas été retiré.

72. La Convention ne précise pas à qui la personne concernée doit s'adresser pour obtenir une confirmation, communication, rectification, etc., ou pour indiquer son opposition ou exprimer son point de vue. Dans la plupart des cas, cependant, il s'agit du responsable du traitement des données ou du sous-traitant qui l'exécute pour son compte. Dans des circonstances exceptionnelles (à des fins de sécurité par exemple), les droits d'accès, de rectification et d'effacement peuvent toutefois être exercé indirectement par l'intermédiaire de l'autorité de contrôle. S'agissant de données relatives à la santé, les droits peuvent également être exercés d'une manière autre que par accès direct, notamment lorsque c'est dans l'intérêt de la personne concernée, avec l'assistance d'un professionnel de santé.

73. Le non-respect d'une objection à un traitement par le responsable du traitement ou par le sous-traitant, le cas échéant (par exemple si le responsable ne cesse pas le traitement ou continue à faire usage des données) a des conséquences juridiques.

74. Alors que le droit d'accès devrait en principe être gratuit, le libellé de la lettre *c* vise à couvrir les différentes hypothèses suivies par les législations nationales, appropriées à chaque cas : communication gratuite à intervalle régulier ou communication moyennant paiement d'une somme forfaitaire plafonnée, etc. Pour garantir un exercice équitable du droit d'accès, l'expression « sous une forme intelligible » s'applique tant au contenu qu'à la forme d'une communication numérique standardisée. Le terme « frais » désigne la redevance à acquitter par l'intéressé, qui doit être raisonnable afin de ne pas empêcher les personnes concernées d'exercer leurs droits et doit en tout cas être égale ou inférieure au coût réel de l'opération.

75. Lorsque des rectifications et effacements sont obtenus conformément au principe énoncé sous *e*, ces rectifications et effacements doivent, chaque fois que possible, être portés à la connaissance des destinataires de l'information originale, à moins que cela ne s'avère impossible ou n'implique des efforts disproportionnés.

76. Concernant l'assistance prévue sous *g / f*, lorsque la personne réside sur le territoire d'une autre Partie, elle doit avoir la faculté de présenter sa demande par l'intermédiaire de l'autorité de contrôle désignée par cette Partie. La demande d'assistance doit contenir toutes les indications nécessaires concernant notamment : le nom, l'adresse et tout autre élément pertinent d'identification concernant le requérant ; le traitement de données auquel la demande se réfère ou le responsable du traitement ; le but de la demande, les éléments en possession du requérant qui permettent de caractériser le traitement concerné. Ce droit peut être limité en application de l'article 9 de la Convention ou aménagé de manière à préserver les intérêts d'une procédure judiciaire pendante.

77. En outre, il est à noter que la détermination de la finalité d'un traitement, les conditions de sa légitimité, le droit de rectification et d'effacement des données, ainsi que la disposition relative à la durée de conservation des données (article 5.3. *e*), associés à un droit effectif d'opposition et au droit de retirer son consentement, offrent un degré de protection efficace aux personnes concernées. Cet ensemble de droits donne effet, de façon pragmatique, à ce qu'il est convenu d'appeler le « droit à l'oubli ».

Article 8 bis – Obligations complémentaires

78. Afin d'assurer un droit effectif à la protection des données à caractère personnel, des obligations complémentaires doivent être prescrites à l'égard des acteurs qui effectuent le traitement des données, à savoir le responsable de traitement et, le cas échéant, le ou les sous-traitants. L'obligation faite au responsable du traitement d'assurer une protection adéquate des données est liée à la responsabilité de vérifier et démontrer que le traitement des données est conforme à la loi applicable. Les principes de protection des données énoncés dans la Convention, qui doivent être appliqués à toutes les étapes du traitement, y compris celle de la conception, sont également un moyen de renforcer la confiance. En particulier, le responsable du traitement et le sous-traitant sont tenus de prendre toutes mesures appropriées, notamment : la formation des employés ; la mise en place de diverses procédures de notification (indiquant par exemple que les données doivent être effacées du système) ; des clauses contractuelles particulières régissant la délégation du traitement et donnant effet à la Convention ; enfin, la mise en place de procédures internes permettant la vérification et la démonstration de la conformité.

79. Il y a lieu de noter, s'agissant de ces obligations complémentaires, qu'une attention particulière a été portée aux exigences imposées aux entreprises certifiées dans le cadre du

système européen des BCR (*Binding Corporate Rules*) et du dispositif CBPR (*Cross Border Privacy Rules system*) de l'APEC.

80. Une des mesures qui pourraient être prises par le responsable du traitement en vue de faciliter la vérification et la démonstration de la conformité serait de désigner un « chargé de la protection des données » disposant des moyens nécessaires à l'accomplissement de sa mission en toute indépendance. Il pourra s'agir d'un agent interne ou externe et sa désignation devra être notifiée à l'autorité de contrôle par le responsable du traitement.

81. Avant d'effectuer un traitement, le responsable du traitement doit procéder à une analyse des risques d'atteinte aux droits et libertés fondamentales des personnes concernées. Les risques doivent également être évalués à l'aune du principe de proportionnalité. Lorsque la présentation détaillée du traitement envisagé (c.-à-d. l'entière description des flux d'information, indiquant quelles données à caractère personnel seront traitées et pour quelles finalités, comment elles seront collectées, l'usage qui en sera fait, les flux internes, les cas où des données pourront être communiquées, les mesures de sécurité, etc.) prévoit les activités d'un sous-traitant, cette obligation peut être imposée au sous-traitant et vient s'ajouter aux obligations du responsable du traitement. L'assistance de développeurs de systèmes d'information (notamment de spécialistes de la sécurité) ou de concepteurs, ainsi que d'usagers et de juristes dans l'analyse des risques serait un avantage et pourrait réduire la charge administrative liée à cet exercice.

82. Afin de mieux garantir un degré de protection efficace, les exigences en matière de protection des données (et donc, par exemple, le choix des logiciels à utiliser compte tenu des impératifs de sécurité) devraient être intégrées dès que possible dans les opérations de traitement, c'est-à-dire, dans l'absolu, au stade de la conception de l'architecture du système. Cet objectif ne doit pas uniquement concerner la technologie employée pour le traitement, mais également les activités liées et les processus de gestion. Des fonctionnalités faciles à utiliser et facilitant la conformité avec les dispositions applicables devraient être en place. Par exemple, l'accès en ligne à leurs propres données personnelles devrait être proposé aux personnes concernées chaque fois que possible, si cela se justifie. Il devrait également y avoir des mécanismes d'usage facile pour que les intéressés puissent transférer leurs données à un autre fournisseur de leur choix ou conserver leurs données eux-mêmes (outils de portabilité des données). Les développeurs et concepteurs d'applications et de logiciels devraient dûment tenir compte du principe de minimisation des données lors de la définition des exigences techniques de la configuration par défaut.

83. Les obligations complémentaires prévues par cet article doivent être constructives et économiquement rationnelles. Elles peuvent être modulées et adaptées en fonction des risques en jeu, de la nature et du volume des données traitées et la taille des responsables des traitements. Des exemptions pourront être prévues pour certaines catégories de traitements, comme ceux ne présentant aucun risque pour les personnes physiques.

Article 9 – Exceptions et restrictions

84. D'une manière générale, aucune exception aux principes de base pour la protection des données à caractère personnel n'est admise. Le bénéfice d'une dérogation est néanmoins permis pour un nombre limité de dispositions, à condition qu'une telle dérogation soit prévue par la loi et nécessaire dans une société démocratique dans des cas particuliers. Les critères définissant une mesure « nécessaire dans une société démocratique » doivent être considérés

à la lumière de la situation prévalant dans chaque pays. Une telle mesure doit cependant poursuivre un but légitime et par conséquent répondre à un « besoin social impérieux » qui ne peut être atteint par des moyens moins intrusifs. Elle doit être proportionnée au but légitime poursuivi et les motifs invoqués par les autorités nationales pour la justifier doivent apparaître « pertinents et suffisants ». Enfin, elle doit être prévue par une loi accessible et prévisible.

85. La nécessité de telles mesures doit être examinée uniquement au regard de buts légitimes limités, comme indiqué aux lettres *a* et *b* du premier paragraphe. La lettre *a* énumère les intérêts majeurs de l'Etat qui peuvent exiger des exceptions. Ces exceptions ont été formulées de façon très précise afin d'éviter que les Etats n'aient une marge de manœuvre trop large en ce qui concerne l'application générale de la Convention.

86. La notion de « sûreté nationale » doit être interprétée de manière restrictive, au sens de la protection de la souveraineté nationale contre des menaces internes ou externes, y compris la protection des relations internationales de l'Etat.

87. L'expression « intérêts économiques et financiers importants de l'Etat » doit être interprétée de manière restrictive et couvre en particulier les exigences de recouvrement de l'impôt et le contrôle des changes. La notion de « prévention et répression des infractions pénales » contenue dans cette lettre comprend les enquêtes et poursuites pénales.

88. La lettre *b* vise les intérêts majeurs des parties privées, ceux de la personne concernée elle-même (par exemple lorsque des intérêts vitaux sont menacés parce que la personne concernée est portée disparue) ou de tiers, comme la liberté d'expression, la confidentialité de la correspondance et des communications (considérée dans chaque cas individuel) et les secrets professionnels ou commerciaux, ainsi que d'autres secrets protégés par la loi.

89. S'agissant des flux transfrontières de données à caractère personnel, une restriction spécifique est autorisée sur le fondement de la liberté d'expression.

90. Le troisième paragraphe donne la possibilité de restreindre les droits dans le cas de certains traitements de données effectués à des fins statistiques ou de recherche scientifique et ne présentant aucun risque pour la protection des données à caractère personnel. Par exemple, l'utilisation de données à des fins statistiques, dans le domaine public comme dans le domaine privé, est possible dans la mesure où ces données sont présentées sous forme agrégée et dissociées de leurs identifiants et sous réserve que des garanties appropriées pour la protection des données soient en place (voir paragraphe 51).

Article 10 – Sanctions et recours

91. Pour que la Convention garantisse un niveau effectif de protection des données, les devoirs des utilisateurs et les droits des personnes concernées devraient être assortis de sanctions et recours correspondants dans la législation nationale des Parties.

92. La détermination de la nature (civile, administrative, pénale / non judiciaire) de ces sanctions, qui doivent être efficaces, proportionnés et dissuasives, devrait être laissée à la discrétion de chaque Partie. Il en va de même pour les voies de recours : les individus doivent avoir la possibilité de contester devant les tribunaux une décision ou une pratique, la définition des modalités du recours étant laissée à la discrétion des Parties. Une indemnisation financière pour tous les dommages, y compris d'ordre moral, provoqués par le traitement des données et des recours collectifs pourraient également être envisagés.

Article 11 – Protection plus étendue

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

Chapitre III – Flux transfrontières de données à caractère personnel

Article 12 – Flux transfrontières

94. Le but de cet article est de faciliter, le cas échéant, la libre circulation de l'information sans considération de frontières (rappelée dans le Préambule) tout en assurant une protection appropriée des personnes à l'égard du traitement des données à caractère personnel.

95. Le régime des flux transfrontières vise à garantir que des informations traitées à l'origine sur un territoire placé sous la juridiction d'une Partie à la Convention (données collectées ou enregistrées dans ce territoire par exemple), puis soumises ultérieurement à la juridiction d'un Etat non partie à la Convention, continueront à faire l'objet d'un traitement conforme à des principes de protection des données appropriés au regard de la présente Convention. L'important est que les personnes concernées à l'origine par les données traitées sur un territoire relevant de la juridiction d'une Partie à la Convention soient toujours protégées par des principes adéquats de protection des données, quelle que soit la loi applicable aux traitements considérés. L'acceptation d'une protection différente dans un contexte international se justifie par le respect dû aux Etats étrangers, qui ont un droit légitime de réglementer autrement la protection des données, et par la nécessité d'éviter d'entraver des relations internationales dans un monde toujours plus intégré. Cette protection différente doit néanmoins être d'une certaine qualité afin de garantir que les droits de l'homme ne soient pas affectés par la mondialisation et la nature transfrontalière des flux de données.

96. La plupart du temps, une telle situation (changement de juridiction et de loi applicable) intervient lorsqu'il y a un transfert de données d'une Partie à la Convention vers un pays étranger. Constitue un transfert de données toute communication ou mise à disposition de données à caractère personnel à un destinataire relevant de la juridiction d'un autre Etat ou autorité.

97. L'article 12 ne s'applique qu'à l'exportation de données et non pas à leur importation. Dans ce dernier cas, en effet, les données sont assujetties au régime de protection des données de l'Etat partie destinataire. Quelques problèmes pourraient par contre se poser en cas de réimportation de données traitées à l'étranger en violation de certaines dispositions du droit de la juridiction d'origine. Dans ce cas, il appartient à la juridiction d'origine (la Partie) de prendre avant l'exportation les mesures nécessaires aux termes de l'article 12.

98. Le paragraphe 1 s'applique aux flux de données entre des Parties à la Convention. Ces flux ne peuvent être interdits ou soumis à une autorisation spéciale, à l'exception des flux de données à caractère personnel concernant des Parties membres d'une organisation régionale et tenues de respecter des règles harmonisées de protection régissant ces flux de données. La raison fondamentale de cette règle est que tous les Etats contractants, dans la mesure où ils ont souscrit au « noyau dur » des dispositions en matière de protection des données énoncé dans

la Convention, offrent un niveau de protection jugé approprié. En l'absence de règles régionales harmonisées et contraignantes régissant les flux de données, les opérations sur les flux de données entre des Parties à la Convention devraient se faire librement.

99. Cette règle ne veut pas dire qu'une Partie ne peut pas prendre d'autres mesures pour s'informer de la circulation de données entre son territoire et celui d'une autre Partie, par exemple des déclarations obligatoires à présenter par les responsables des traitements. Cependant, de telles mesures ne doivent pas être utilisées par une Partie comme un moyen d'avoir accès aux données à caractère personnel de personnes relevant de sa juridiction.

100. Il peut arriver dans certains cas que des flux de données partent simultanément d'une Partie vers plusieurs organisations internationales ou pays étrangers, dont certains sont parties à la Convention et d'autres non. Dans de tels cas, la Partie à l'origine du transfert de données, qui a une procédure d'exportation pour les Etats non contractants, ne pourra pas toujours éviter que cette procédure soit appliquée également aux données destinées à une autre Partie, mais dans ce cas elle devra procéder de façon à assurer que la procédure pour les transferts de données vers cette dernière Partie soit dûment autorisée.

101. Le paragraphe 2 réglemente les flux transfrontières de données vers un destinataire qui n'est pas soumis à la juridiction d'une Partie. Comme pour tout transfert de données à travers les frontières nationales, un niveau approprié de protection dans l'Etat ou l'organisation destinataire doit être assuré. Dans la mesure où ceci ne saurait être présumé puisque le destinataire n'est pas une Partie, la Convention établit deux grands moyens susceptibles de garantir que le niveau de protection est bien approprié : les règles de droit ou des garanties standardisées approuvées ou ad hoc, juridiquement contraignantes, ayant force exécutoire et dûment mises en œuvre.

102. Un niveau approprié de protection des données peut être assuré si les personnes (morales ou physiques) participant au transfert fournissent des garanties suffisantes, comme des garanties standardisées et approuvées liant à la fois le responsable du traitement qui transfère les données et le destinataire non soumis à la juridiction d'une Partie. L'adoption de garanties standardisées communes aux Parties à la Convention devrait être recherchée.

103. Le contenu de ces contrats doit inclure les éléments pertinents en matière de protection des données. En outre, du point de vue formel, les clauses contractuelles pourraient, par exemple, prévoir que la personne concernée dispose d'un interlocuteur au sein du personnel du responsable des flux de données, qui serait chargé de veiller au respect des normes matérielles de protection. Elle pourrait le contacter à tout moment et sans frais en lien avec les traitements ou les flux de données et, le cas échéant, obtenir son aide pour l'exercice de ses droits.

104. Le niveau de la protection devrait être évalué au cas par cas, pour chaque transfert ou catégorie de transfert. Plusieurs éléments du transfert doivent être examinés, en particulier : la nature des données, les finalités et la durée des traitements pour lesquels les données sont transférées, le respect des règles de droit du pays de destination finale, les règles de droit, générales et sectorielles applicables dans l'Etat ou l'organisation en question et les règles professionnelles et de sécurité qui y sont applicables.

105. L'appréciation du niveau approprié de protection doit prendre en considération les principes de la Convention et la manière dont ils sont respectés dans le pays ou l'organisation destinataires – dans la mesure où ils sont pertinents dans le cas concret – ainsi que la façon dont la personne concernée peut défendre ses intérêts en cas de non-conformité. Une

évaluation peut de la même façon être effectuée pour l'ensemble d'un Etat ou d'une organisation, permettant ainsi tout transfert de données vers cette destination. Dans ce cas, le niveau approprié de protection est déterminé par l'autorité de contrôle compétente de chaque Partie.

106. Le paragraphe 4 permet aux Parties de déroger, dans des cas particuliers, au principe selon lequel un niveau approprié de protection doit être assuré et d'autoriser un transfert donné vers un destinataire n'assurant pas une telle protection. De telles dérogations ne sont permises que dans des circonstances bien définies (consentement ou intérêt spécifique de la personne concernée, existence d'intérêts légitimes prépondérants et prévus par la loi). Elles doivent également faire l'objet d'une surveillance de la part de l'autorité de contrôle compétente. De telles dérogations ne doivent pas être disproportionnées et ne doivent pas être utilisés pour des transferts massifs ou répétitifs.

107. Le paragraphe 5 prévoit une garantie complémentaire, à savoir que l'autorité de contrôle compétente a la faculté d'exiger que la qualité et l'efficacité des mesures prises soient démontrées ainsi que d'interdire, suspendre ou soumettre à condition le transfert. Dans le cas particulier de garanties ad hoc, l'autorité de contrôle compétente est informée des modalités du transfert.

108. A l'avenir, les flux de données et la nécessaire protection appropriée des données pourraient s'appuyer de plus en plus sur les avantages d'une articulation plus étroite des cadres de protection de la vie privée existant à travers le monde, comme les BCR de l'Union européenne, les lignes directrices de l'OCDE ou le cadre de l'APEC relatif à la protection de la vie privée et ses organismes certificateurs CBPR.

Chapitre III bis Autorités de contrôle

Article 12 bis – Autorités de contrôle

109. La mise en œuvre effective des principes de la Convention requiert l'adoption de sanctions et de recours appropriés (article 10). La plupart des pays disposant d'une loi en matière de protection des données ont institué à cet égard une autorité de contrôle des traitements de données à caractère personnel pour aborder les enjeux de ce domaine complexe, en perpétuelle évolution, à la lumière des dynamiques organisationnelles, sociales et sociétales. Ce contexte exige un regard extérieur impartial, une grande réactivité comparée à la lenteur du système judiciaire et une expertise spécialisée par rapport à d'autres acteurs externes tels que les actions parlementaires. Il s'agit généralement d'un commissaire, d'une commission, d'un médiateur ou d'un inspecteur général. Pour fournir un recours approprié, ces autorités de contrôle dans le domaine de la protection des données doivent être dotées de pouvoirs et de compétences effectives et jouir d'une réelle indépendance dans l'exercice de leur mission. Elles sont une composante essentielle du système de contrôle de la protection des données dans une société démocratique.

110. Cet article de la Convention vise à renforcer la protection effective de l'individu en rendant nécessaire la création d'une ou plusieurs autorités de contrôle qui contribuent à la protection des droits et libertés de l'individu à l'égard du traitement des données à caractère personnel. Plus d'une autorité pourrait être nécessaire pour satisfaire les particularités des différents systèmes juridiques (Etats fédéraux par exemple). Ces autorités pourraient exercer leurs fonctions sans préjudice de la compétence des juridictions ou autres instances chargées de veiller au respect du droit interne donnant effet aux principes de la Convention. Les autorités de

contrôle devraient pouvoir disposer de ressources humaines (juristes, informaticiens) et techniques appropriées pour agir rapidement et efficacement.

111. Les Parties disposent d'une marge d'appréciation considérable quant aux modalités de création et de fonctionnement de ces autorités pour qu'elles puissent mener à bien leur mission. Selon la Convention, toutefois, ces autorités devraient être dotées au moins de pouvoirs d'investigation et d'intervention. Elles devraient en outre être consultées sur les processus normatifs législatifs et administratifs relatifs à la protection des données, être dotées de pouvoirs spécifiques dans le contexte des flux de données, pouvoir être saisies de plaintes déposées par des particuliers (et les traiter par ordre de priorité), être dotées du pouvoir de prononcer des décisions et d'imposer des sanctions administratives, ainsi que du pouvoir d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente toute violation des dispositions pertinentes. Elles devraient enfin avoir une mission de sensibilisation à la protection des données.

112. Les autorités de contrôle devraient être dotées de pouvoirs d'investigation, tels que la possibilité de demander au responsable du traitement et au sous-traitant des informations concernant des traitements de données à caractère personnel et de les obtenir. En vertu de l'article 8 de la Convention, de telles informations doivent être mises à disposition, notamment dans les cas où l'autorité de contrôle est saisie par une personne voulant exercer ses droits prévus en droit interne.

113. En ce qui concerne les pouvoirs d'intervention – notamment à l'égard de traitements qui présentent des risques particuliers au regard des intérêts et des droits et libertés fondamentales d'une personne physique –, ceux-ci peuvent prendre de multiples formes en droit interne. A titre d'exemple, l'autorité de contrôle pourrait avoir la possibilité d'obliger d'office le responsable du traitement à rectifier, effacer ou détruire des données collectées de manière illégale, si la personne concernée n'est pas en mesure d'exercer ces droits personnellement. La possibilité de solliciter une ordonnance d'injonction contre les responsables de traitements qui ne sont pas prêts à communiquer les informations requises dans des délais raisonnables constituerait une transposition particulièrement efficace du pouvoir d'intervention. Ce pouvoir d'intervention pourrait enfin englober la possibilité de rendre des avis préalables à la mise en œuvre des opérations de traitement (lorsque le traitement présente des risques particuliers au regard des droits et libertés fondamentales, l'autorité de contrôle devrait être consultée par les responsables de traitement dès les tout premiers stades de la conception du traitement) ou bien de saisir les parlements nationaux ou d'autres institutions étatiques.

114. Tout en contribuant à la protection des droits individuels, l'autorité de contrôle sert d'intermédiaire entre la personne concernée et le responsable du traitement. Dans ce contexte, il semble particulièrement important que l'autorité de contrôle puisse fournir des informations aux individus ou aux responsables de traitement de données et aux sous-traitants sur les droits et obligations en matière de protection des données.

115. En outre, toute personne devrait avoir la possibilité de demander à l'autorité de contrôle de mener les enquêtes nécessaires sur toute plainte concernant ses droits et libertés à l'égard de traitements de données à caractère personnel. Cela contribue à garantir le droit de disposer d'un recours approprié tel que prévu à l'article 10 et à l'article 8 de la Convention. Outre ces investigations, l'autorité de contrôle peut notamment décider d'imposer une sanction administrative ou, si elle ne dispose pas de ce pouvoir, de saisir du dossier une autre autorité compétente dotée de ce pouvoir. Dans certaines juridictions, les autorités de contrôle n'ont pas qualité pour ester en justice et le pouvoir d'imposer des sanctions administratives est donc très

important pour leurs capacités en matière d'application des lois. Lorsque de tels pouvoirs sont conférés aux autorités de contrôle, il importe de leur fournir les ressources nécessaires à l'accomplissement de leur mission.

116. Dans les cas où une décision administrative produit des effets juridiques, toute personne concernée est en droit de disposer d'un recours juridictionnel. Néanmoins, le droit interne peut soumettre ce recours juridictionnel à une saisine préalable de cette autorité.

117. Les Parties devraient accorder à l'autorité de contrôle le pouvoir, soit d'ester en justice, soit de porter à la connaissance de la justice toute violation aux principes de la protection des données. Ce pouvoir dérive notamment du pouvoir de mener des investigations qui peuvent conduire l'autorité à constater une violation aux droits des personnes. L'obligation des Parties d'accorder à l'autorité ce pouvoir peut être remplie en lui donnant le pouvoir de prendre des décisions.

118. La liste des pouvoirs attribués à l'autorité de contrôle par l'article 12 bis n'est pas exhaustive. Il convient donc de rappeler que les Parties ont d'autres possibilités de donner effet à la mission de l'autorité de contrôle. A titre d'exemple, elle pourrait être saisie d'une plainte d'une association, en particulier lorsque les droits des personnes représentées par cette dernière sont limités en vertu de l'article 9 de la Convention. L'autorité pourrait tenir un registre des traitements ouvert au public. Elle pourrait aussi être appelée à donner son avis lors de l'élaboration de mesures législatives, réglementaires ou administratives relatives au traitement de données à caractère personnel ou sur des propositions de codes de conduite.

119. Les autorités de contrôle ne sont en mesure de garantir efficacement les droits individuels et les libertés que si elles exercent leurs fonctions en toute indépendance. Un faisceau d'éléments contribue à garantir l'indépendance de l'autorité de contrôle dans l'exercice de ses fonctions. Parmi ces éléments on peut citer la composition de l'autorité, le mode de désignation de ses membres, la possibilité donnée à ses membres de participer à des réunions sans autorisation ou instruction, la possibilité de consulter des experts techniques ou autres ou d'organiser des consultations externes, la durée et les conditions de cessation des fonctions d'un membre, l'octroi à l'autorité de ressources suffisantes ou la possibilité de prendre des décisions sans recevoir d'ordres de l'extérieur ni être soumise à des injonctions.

120. L'interdiction de solliciter ou accepter des instructions ne couvre que l'accomplissement de leurs tâches en tant qu'autorités de contrôle, et non pas lorsqu'elles agissent en tant qu'employeur par exemple. Ceci n'empêche pas les autorités de contrôle de solliciter des avis (par exemple auprès de consultants, d'homologues, etc.) dans les cas où elles l'estiment nécessaire, pour autant qu'elles portent un jugement indépendant.

121. La transparence concernant les travaux et activités des autorités de contrôle devrait être encouragée, en particulier par la publication de rapports d'activité annuels comportant, entre autres, des informations relatives aux mesures prises pour faire appliquer la loi. L'autorité de contrôle devrait pouvoir informer l'opinion par des rapports réguliers, la publication de ses avis ou par tout autre moyen de communication, et formuler publiquement des recommandations au chef de l'Etat et au parlement en vue d'améliorer le système de protection des données.

122. En contrepartie de cette indépendance, les décisions des autorités de contrôle doivent elles-mêmes pouvoir faire l'objet d'un recours juridictionnel, conformément au principe de légalité et de la prééminence du droit.

123. En outre, dans les cas où l'autorité de contrôle ne dispose pas elle-même de compétences juridictionnelles, l'intervention d'une autorité de contrôle ne doit pas empêcher la personne concernée d'exercer un recours juridictionnel.

124. Le renforcement de la coopération entre les autorités de contrôle contribuerait au développement du niveau de protection accordé par les Parties en vertu de la Convention. Cette coopération est complémentaire à l'entraide entre les Parties en vertu du chapitre IV de la Convention et aux travaux du comité conventionnel. Elle vise à une meilleure protection des personnes concernées. Ces personnes sont en effet de plus en plus souvent directement touchées par des traitements de données qui ne se bornent pas à un seul pays et qui concernent alors les lois et autorités de plusieurs pays. On peut ainsi citer, à titre d'exemple, le développement des réseaux électroniques internationaux, le nombre croissant de flux transfrontières en matière de prestation de services ou dans le milieu du travail. Dans ce contexte, la coopération internationale des autorités de contrôle assure que les individus peuvent exercer leurs droits au niveau international comme au niveau national. La promotion de la coopération pourrait prendre la forme de réseaux ou de réunions, en tirant parti des possibilités déjà existantes de réunion des Parties pour débattre de questions d'intérêt commun. L'importance, pour ces autorités, de se tenir au courant des évolutions technologiques sera soulignée. Toutes les fois qu'une autorité souhaitera élaborer des recommandations générales, elle pourra décider de consulter les acteurs concernés.

Chapitre IV – Entraide

Article 13 – Coopération entre les Parties

125. Les autorités de contrôle se prêteront mutuellement une assistance générale pour les contrôles a priori (par exemple en vue de certifier que les points d'accès situés dans un pays et reliés à un autre pays sont bien conformes aux règles de sécurité des données) et une assistance spécifique pour les contrôles a posteriori (par exemple en vue de vérifier les activités d'un centre de traitement particulier). Les informations échangées pourront être de caractère juridique ou factuel.

126. Cette coopération ne devrait en rien nuire aux instruments de coopération existants en matière civile et pénale.

Article 14 (biffé)

Article 15 – Garanties concernant l'assistance

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

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

Article 16 – Refus de demandes d'assistance

129. Cet article pose le principe selon lequel les Parties sont tenues de donner suite aux demandes d'assistance. Les motifs de refus sont ensuite énumérés de manière exhaustive. Ils correspondent d'une manière générale à ceux prévus par d'autres conventions internationales d'entraide.

130. L'expression « exécution » utilisée à la lettre *c* doit s'entendre dans un sens large couvrant non seulement la réponse à la demande, mais aussi l'activité qui la précède. Par exemple, une autorité requise pourrait refuser d'agir non seulement si la transmission à l'autorité requérante de l'information demandée pouvait porter préjudice aux droits et libertés fondamentales d'un individu, mais également si le fait même de rechercher l'information constituait un risque d'atteinte à ces droits et libertés fondamentales.

Article 17 – Frais et procédures de l'assistance

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

132. La notion d'« experts » au sens du paragraphe 1 comprend notamment les informaticiens dont on demande l'intervention pour effectuer des tests sur l'ordinateur ou contrôler la sécurité d'un traitement.

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

Chapitre V – Comité conventionnel

134. Le but des articles 18, 19 et 20 est de faciliter l'application de la Convention et, le cas échéant, de perfectionner celle-ci.

135. Un comité conventionnel composé de représentants de toutes les Parties, issus des autorités de contrôle nationales et du gouvernement, s'efforcera de formuler des propositions ou de donner des avis à ces Parties en vue de la solution de ces problèmes. / des problèmes soulevés / en vue de résoudre tout problème éventuel.

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

137. Puisque la Convention aborde un domaine en perpétuelle évolution, on peut s'attendre à ce que des questions se posent tant en ce qui concerne l'application pratique de la Convention (article 19, lettre *a*) que pour ce qui est de son interprétation (même article, lettre *d*).

138. Conformément à l'article 21, le comité conventionnel a la faculté de proposer des amendements à la Convention et d'examiner d'autres propositions formulées par une Partie ou par le Comité des Ministres (article 19 lettres *b* et *c*).

139. Pour garantir la mise en œuvre des principes de protection des données consacrés par la Convention et assurer un niveau harmonisé de protection entre les Parties à la Convention, le comité conventionnel jouera un rôle clé dans l'évaluation du respect de la Convention, notamment en préparant une évaluation du niveau de protection des données offert par un candidat à l'adhésion (article 19 lettre e*),* ou en examinant périodiquement l'application de la Convention par les Parties (article 19 lettre *h*). Le comité conventionnel aura également la faculté d'examiner la conformité du régime de protection des données d'un Etat ou d'une organisation internationale avec la Convention (article 19 lettre *f*).

140. En fournissant de tels avis sur le degré de conformité avec la Convention, le comité conventionnel conduira ses travaux sur la base d'une procédure équitable, transparente et publique décrite dans son règlement.

141. De surcroît, le comité conventionnel aura la faculté d'approuver des modèles de garanties standardisées pour les transferts de données (article 19 lettre *g*).

142. Enfin, le comité conventionnel pourra contribuer au règlement de toute difficulté surgissant entre les Parties (article 19 lettre *i*). En ce qui concerne les modes de règlement amiable des différends, le comité conventionnel s'efforcera de parvenir à un règlement par la négociation ou tout autre moyen pacifique.

Chapitre VI – Amendements

Article 21 – Amendements

143. Le Comité des Ministres, qui a adopté le texte original de cette Convention, est également compétent pour l'approbation de tout amendement.

144. Conformément au paragraphe 1, des amendements peuvent être proposés à l'initiative du Comité des Ministres lui-même, du comité conventionnel ou d'une Partie (qu'il s'agisse ou non d'un Etat membre du Conseil de l'Europe).

145. Toute proposition d'amendement ne provenant pas du comité conventionnel doit lui être soumise pour avis aux termes du paragraphe 3.

Chapitre VII – Clauses finales

Article 22 – Entrée en vigueur

146. Etant donné qu'un large champ d'application géographique est jugé essentiel pour l'efficacité de la Convention, le paragraphe 2 fixe à cinq le nombre de ratifications d'Etats membres du Conseil de l'Europe nécessaires pour son entrée en vigueur.

Article 23 – Adhésion d'Etats non membres et d'organisations internationales

147. La Convention, qui a été élaborée en collaboration étroite avec l'OCDE et plusieurs Etats non européens membres de cette organisation, est ouverte à tout pays du monde satisfaisant à ses dispositions. Le comité conventionnel est chargé de la tâche d'évaluer la conformité et de préparer un avis à l'intention du Comité des Ministres concernant le degré de protection des données du candidat à l'adhésion.

148. Etant donné que les flux de données ne connaissent pas de frontières, l'adhésion de pays et d'organisations internationales du monde entier est recherchée.

Article 24 – Clause territoriale

149. L'application de la Convention à des territoires lointains placés sous la juridiction des Parties ou au nom desquels une Partie peut s'engager revêt une importance pratique au vu de l'utilisation qui est faite de pays éloignés pour des opérations de traitement de données, pour des raisons de coût et de main-d'œuvre, ou au vu de l'utilisation de la capacité de traitement en alternance jour/nuit.

Article 25 – Réserves

150. Les règles contenues dans cette Convention constituent les éléments les plus fondamentaux et essentiels pour une protection efficace des données. C'est pourquoi la Convention n'admet aucune réserve. Ses dispositions offrent néanmoins une souplesse raisonnable compte tenu des dérogations admises par certains articles.

Article 26 – Dénonciation

151. Conformément à la Convention de Vienne sur le droit des traités, l'article 80 autorise toute Partie à dénoncer la Convention.

Article 27 - Notifications

152. Ces dispositions sont conformes aux clauses finales habituelles contenues dans d'autres conventions du Conseil de l'Europe.