2 juin 2016

CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL [STE N° 108]

PROJET DE RAPPORT EXPLICATIF

Le présent document a été préparé à partir du texte consolidé des propositions de modernisation de la Convention 108 : la numérotation des articles ne correspond pas au projet de protocole portant modification de la Convention.

I. INTRODUCTION

Contexte

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 « Convention 108 ») a décidé à sa 25e réunion plénière (2-4 septembre 2009) de fixer comme première priorité de son « Programme de travail pour 2009 et les années à venir » la préparation d'amendements à la Convention 108.

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

Les priorités proposées ont été officiellement approuvées par le Comité des Ministres en mars 2010, lorsque les Délégués des Ministres (à leur 1079e réunion, le 10 mars 2010) ont salué l'adoption du programme de travail du T-PD et encouragé ce dernier à lancer le travail de 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 quant à eux 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 s'est elle aussi félicitée de l'initiative 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 ».

Dans un premier temps, le T-PD a chargé des experts d'établir un rapport[1] en vue de recenser les domaines dans lesquels une modernisation de la Convention 108 serait nécessaire pour répondre aux nouveaux défis posés par les technologies de l'information et de la communication.

Un deuxième rapport[2] a ensuite été préparé pour aborder un autre aspect essentiel de la modernisation, à savoir l'évaluation de la mise en œuvre par les Etats contractants de la Convention 108.

[1] Rapport sur les lacunes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) 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 Gyzeghem du CRIDS Namur.

[2] Rapport sur les modalités et les mécanismes d'évaluation de la mise en œuvre et du suivi de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère

A partir du premier rapport, le T-PD a élaboré une liste de questions à examiner dans le cadre du travail de modernisation de la Convention, ainsi qu'un document de consultation[3] comportant 30 questions.

Une consultation publique sur ces 30 questions a été lancée en vue 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). Elle visait à permettre à tous les acteurs concernés (particuliers, société civile, secteur privé, organismes de surveillance, autorités de contrôle) du monde entier de donner leur point de vue sur l'avenir de la Convention 108.

De nombreuses contributions ont été reçues du secteur public (autorités gouvernementales et autorités de protection des données), du secteur privé (secteur bancaire, assurances, commerce électronique, marketing, distribution audio-visuelle, recherche socio-économique, etc.), des milieux universitaires et des associations intéressées. Les réponses obtenues provenaient de plusieurs continents et pas uniquement d'Europe.

Trois réunions du Bureau du T-PD ont été nécessaires en 2011 pour transformer ce matériel dense et extrêmement riche[4] en propositions concrètes de modernisation[5] de la Convention 108, lesquelles ont été examinées en première lecture à la 27e réunion plénière du T-PD (30 novembre - 2 décembre 2011).

Sur la base des discussions tenues à cette 27e réunion plénière et des projets de documents soumis par la suite pour commentaires, des versions révisées[6] des propositions de modernisation ont été préparées par le Bureau du T-PD. Outre le T-PD, les projets successifs ont été présentés pour commentaires à divers comités du Conseil de l'Europe ainsi qu'à des acteurs du secteur privé et de la société civile (en particulier à l'occasion d'un échange de vues tenu le 2 mai 2012 au Bureau du Conseil de l'Europe à Bruxelles).

A sa 28e réunion plénière (19-22 juin 2012), le T-PD a examiné en deuxième lecture les propositions de modernisation de la Convention 108[7] et chargé son Bureau de finaliser les propositions à la lumière des échanges tenus et des commentaires formulés, en vue de leur examen à sa 29e réunion plénière (27-30 novembre 2012).

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

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

Le 10 juillet 2013, à leur 1176e réunion, les Délégués des Ministres ont pris note du travail réalisé par le T-PD en vue de moderniser la Convention 108 et approuvé le mandat du CAHDATA pour permettre la poursuite de ces travaux.

---

personnel (STE n° 108) et de 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_FR.pdf

[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 and 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 CAHDATA a tenu trois réunions, une en 2013 (12 - 14 novembre 2013) et deux en 2014 (28 - 30 avril 2014 et 1-3 décembre 2014). A sa première réunion, le CAHDATA a procédé à une lecture complète des propositions de modernisation adoptées par le Comité consultatif en novembre 2012, ce qui a abouti à la production d'un nouveau document de travail pour sa deuxième réunion.

Au cours de ses deuxième et troisième réunions, le CAHDATA a examiné article par article les propositions de modernisation et y a introduit des amendements, modifications rédactionnelles et autres corrections. Le comité ad hoc a approuvé le texte de la Convention modernisée à sa 3e réunion[12] et chargé le Secrétariat de préparer le projet de Protocole portant modification de la Convention 108. Ce projet de Protocole a été transmis, avec son rapport explicatif, au Comité des Ministres pour examen et adoption.

En 2016, ...

Modernisation : objectifs et principales caractéristiques

Chaque jour apporte son lot de nouvelles menaces pour les droits de l'homme et les libertés fondamentales, et notamment le droit à la vie privée. Il est devenu évident que la Convention 108 devait être modernisée pour mieux répondre aux nouveaux défis en matière de protection de la vie privée découlant de l'utilisation croissante des nouvelles technologies de l'information et de la communication, de la mondialisation des opérations de traitement et des flux toujours plus importants de données à caractère personnel, tout en renforçant le mécanisme d'évaluation et de suivi de la Convention.

Les contributions reçues dans le cadre de la consultation publique de 2011 et des discussions ultérieures dans divers contextes ont fait apparaître un large consensus selon lequel il convenait de maintenir la nature générale et technologiquement neutre des dispositions de la Convention, de préserver la cohérence et la compatibilité de la Convention avec d'autres cadres juridiques et de réaffirmer son caractère ouvert, qui lui donne un potentiel unique d'instrument à vocation universelle. Le texte de la Convention est de nature générale et peut être complété par des textes sectoriels plus détaillés et non contraignants, par exemple des Recommandations du Comité des Ministres élaborées avec la participation des parties intéressées.

La modernisation de la Convention est une question qui est particulièrement d'actualité compte tenu de la nécessité de veiller à ce que des principes fondamentaux communs garantissent dans le plus grand nombre possible de pays du monde un niveau adéquat de protection des personnes physiques à l'égard du traitement automatisé des données à caractère personnel, face à l'internationalisation croissante du traitement de ces données (flux de données omniprésentes) et à l'incertitude juridique qui en découle quant au droit applicable.

Une plus grande harmonisation des lois relatives à la protection des données dans le monde pourra être obtenue en multipliant le nombre d'adhésions à la Convention 108.

La modification des traités internationaux est régie par le droit général des traités, dont l'un des principaux instruments est la Convention de Vienne de 1969 sur le droit des traités. Cette Convention prévoit que l'amendement des traités repose sur le consentement des Parties. Son article 39 dispose qu'un traité « peut être amendé par accord entre les Parties », mais ne prévoit pas de formalités particulières pour l'expression de cet accord. La modification d'un traité ne requiert pas l'adoption d'un autre traité sous une forme écrite. Dans son commentaire relatif à l'article 39 de la Convention de Vienne, la Commission du droit international a affirmé que les amendements peuvent également être adoptés par accord verbal, voire tacite. Au sein du Conseil de l'Europe, il est pratique courante de modifier les conventions par l'adoption de protocoles portant amendement à ces conventions, lesquels entrent généralement en vigueur après acceptation ou ratification par l'ensemble des Parties à la Convention.

La Convention 108 et les autres cadres internationaux

[12] 3e réunion du CAHDATA (1-3 décembre 2014).

Organisation de coopération et de développement économiques (OCDE) - 1980

La coopération qui avait présidé à la rédaction de la Convention du Conseil de l'Europe et des Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel a été renouvelée lors des exercices parallèles de modernisation de la Convention et de révision[13] des Lignes directrices de 1980. Les deux organisations ont entretenu des liens étroits tant au niveau du secrétariat que des comités (participation aux réunions avec le statut d'observateur) en vue de conserver la compatibilité entre les deux textes.

Organisation des Nations Unies - 1990

Les Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel (1990) ont dûment été pris en compte.

Union européenne (UE) - 1995

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 94/46/CE ») est rédigé 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 ; »

Bien que la Directive se soit fortement inspirée de la Convention 108 et vise à préciser et amplifier les principes qui y sont énoncés, elle n'est pas identique à cette dernière. La cohérence et la compatibilité des deux cadres doivent être préservées à l'avenir. De ce point de vue, les dispositions de la Convention 108 et les propositions de modernisation, de nature générale, pourront certainement continuer d'être précisées et amplifiées par le cadre juridique proposé par l'Union européenne, en prenant dûment en considération les spécificités de chaque système.

En ce qui concerne les flux transfrontières de données, l'articulation entre les deux régimes devra être assurée à l'avenir pour garantir leur compatibilité et leur complémentarité, ainsi que la nécessaire protection des personnes physiques dans chacun d'entre eux. Le fait qu'un Etat soit partie à la Convention 108 pourra être pris en compte lors de l'évaluation par l'Union européenne de l'adéquation du niveau de protection offert par cet Etat.

Dans ses priorités pour la coopération[14] avec le Conseil de l'Europe en 2014-2015, l'Union européenne a inscrit la protection des données au nombre des domaines thématiques prioritaires pour « soutenir la diffusion, à l'échelle mondiale, des règles édictées par cette convention ».

Coopération économique pour l'Asie-Pacifique (APEC) - 2004

Le cadre de l'APEC relatif à la protection de la vie privée et son système de règles transfrontalières de protection de la vie privée (*Cross Border Privacy Rules*, CBPR) ont été pris en considération dans la réflexion sur la nécessité de renforcer la coopération entre régions et régimes de protection, notamment en ce qui concerne leur application au niveau international et les flux transfrontières de données.

[13] La Recommandation révisée concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel a été adoptée par le Conseil de l'OCDE le 11 juillet 2013.

[14] Document « Priorités de l'UE pour la coopération avec le Conseil de l'Europe en 2014-2015 » du 7 novembre 2013, référence15857/13.

Autres instruments

Enfin, une attention particulière a également été portée aux normes internationales sur la protection de la vie privée à l'égard du traitement des données à caractère personnel, approuvées par la Conférence internationale des commissaires à la protection des données et à la vie privée (Madrid, 2009).

II. 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 trente ans, la Convention 108 est devenue la clé de voûte du cadre juridique international en matière de protection des données dans plus de 40 pays européens. Elle influence également les politiques et les législations bien au-delà des frontières de l'Europe. Le Conseil de l'Europe modernise la Convention pour faire face aux nouveaux défis qui se posent en matière de protection des données du fait des évolutions technologiques, économiques et sociales dans la société de l'information et de la communication, ainsi que de l'internationalisation 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 qui ont conduit à l'adoption de ces deux instruments. Ces rapports doivent être lus conjointement avec le présent document pour ces aspects particuliers.

4. Les travaux de modernisation s'inscrivent dans le cadre plus général de plusieurs réformes parallèles des instruments internationaux de protection des données ; il ont tenu dûment compte des Lignes directrices de 1980 de l'Organisation de coopération et de développement économiques (OCDE) sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, des Principes directeurs de 1990 des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel, du cadre de l'Union européenne (à partir de 1995), du cadre relatif à la protection de la vie privée de la Coopération pour l'Asie-Pacifique (2004) et des Normes internationales de 2009 sur la protection de la vie privée à l'égard du traitement des données à caractère personnel[15].

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 à sa 29e réunion plénière (27-30 novembre 2012) et soumises au Comité des Ministres qui a ensuite chargé le CAHDATA de les finaliser. Ce travail a été terminé à l'occasion de la 3e et dernière réunion du CAHDATA (1-3 décembre 2014). Après la finalisation du cadre de l'UE en matière de protection des données le 15 décembre 2015, un autre CAHDATA a été établi pour examiner les questions en suspens.

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

Préambule

[15] Saluées par la 31e Conférence internationale des commissaires à la protection des données et à la vie privée, tenue à Madrid le 5 novembre 2009.

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

8. Un objectif majeur de la Convention est de mettre les individus en position de connaître, comprendre et contrôler le traitement de leurs données à caractère personnel par des tiers. C'est pourquoi le préambule mentionne expressément le droit à l'autonomie personnelle, le droit de chacun de contrôler ses propres données à caractère personnel, lequel découle en particulier du droit au respect de la vie privée, ainsi que la dignité de la personne. La dignité 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 ou produits de consommation. Par conséquent, des mesures et décisions ayant des conséquences importantes sur une personne et prises uniquement sur le fondement d'un traitement automatisé de données, ne sauraient être rendues définitives si la personne concernée n'a pas le droit de faire valoir son point de vue.

9. Eu égard au rôle que joue le droit à la protection des données à caractère personnel dans la société, le préambule souligne qu'il convient de concilier les intérêts, droits et libertés fondamentales des individus et que le droit à la protection des données à caractère personnel est à considérer avec ces intérêts, droits et libertés fondamentales, dont la liberté d'expression. Il convient de ménager un juste équilibre entre les intérêts, droits et libertés en jeu afin de ne pas indûment restreindre l'un d'entre eux. 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 confirme en outre que l'exercice du droit à la protection des données, qui n'est pas absolu, ne saurait être utilisé de manière générale pour empêcher l'accès du public aux documents publics[16].

10. La Convention 108, à travers les principes qu'elle énonce et les valeurs qu'elle contient, protège l'individu et définit un cadre approprié pour la circulation des informations. Ce point est important car les flux internationaux d'informations sont une caractéristique importante de la société, qui permet l'exercice des droits et libertés fondamentaux tout en suscitant l'innovation et en encourageant le progrès social et économique. La circulation des données à caractère personnel dans une société de l'information et de la communication doit se faire dans le respect des droits des individus. Ces droits doivent également être respectés lors de l'utilisation de technologies innovantes. Cela permet de renforcer la confiance dans l'innovation et les nouvelles technologies et partant, de continuer à favoriser leur développement.

11. La coopération internationale entre les autorités de contrôle étant un élément clé de la protection efficace des personnes, la Convention vise à renforcer cette coopération, notamment en permettant aux Parties de se prêter mutuellement assistance et en fournissant la base juridique appropriée pour l'établissement d'un cadre de coopération et d'échange d'informations à des fins d'enquête et d'application des lois.

Chapitre I - Dispositions générales

Article 1 – Objet et but

12. Le premier article décrit l'objet et le but de la Convention. Il 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 particulière, en premier lieu dans 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 »[17]. Il a également été consacré comme un droit fondamental à l'article 8 de la Charte des droits fondamentaux de l'Union européenne ainsi que dans les

[16] Voir Convention du Conseil de l'Europe sur l'accès aux documents publics (STCE n° 205).
[17] Cour européenne des droits de l'homme, *MS c. Suède* 1997 par. 41.

constitutions de plusieurs Parties à la Convention. Le droit à la protection des données à caractère personnel n'est pas un droit isolé ; au contraire, c'est un droit sans lequel il ne serait pas possible de jouir et d'exercer de la même manière d'autres droits et libertés fondamentales, comme le droit au respect de la vie privée, la liberté d'expression, la liberté d'association, la liberté de circulation et le droit à un procès équitable.

13. Les garanties énoncées dans la Convention s'étendent à toute personne physique, indépendamment de sa nationalité ou de son lieu de résidence. Aucune discrimination entre les citoyens d'un pays et les ressortissants de pays tiers n'est autorisée dans l'application de ces garanties[18]. Des clauses restreignant la protection des données aux ressortissants d'un Etat ou aux étrangers résidant légalement sur son territoire sont donc incompatibles avec la Convention.

Article 2 – Définitions

14. Les définitions figurant dans la présente Convention sont conçues pour favoriser une application uniforme des termes traduisant certains concepts fondamentaux dans les législations nationales.

Lettre a – « données à caractère personnel »

15. On entend par « personne identifiable » une personne qu'il est possible d'identifier directement ou indirectement. Une personne physique n'est pas considérée comme « identifiable » si son identification nécessite des délais, des activités ou des moyens déraisonnables. Tel est le cas lorsque l'identification de la personne concernée exige des opérations excessivement complexes, longues et coûteuses ou la violation, sanctionnée pénalement, d'une obligation légale de secret (par exemple, un médecin qui violerait le secret médical pour révéler le nom d'un patient dissimulé par un code dans un contexte de recherche). Ce qui constitue des « délais, des activités ou des moyens déraisonnables » peut évoluer en fonction des progrès technologiques et autres et devra être déterminé au cas par cas compte tenu de l'objet du traitement et de critères objectifs tels que le coût, les bénéfices d'une telle identification, le type de responsable du traitement, la technologie employée, etc.

16. Le terme « identifiable » ne fait pas uniquement référence à l'identité civile ou juridique en tant que telle de la personne, mais également à tout élément susceptible d'« individualiser » ou de distinguer (et donc de traiter différemment) une personne parmi d'autres. Cette « individualisation » pourrait se faire, par exemple, à partir d'un numéro d'identification, d'un pseudonyme, de données biométriques ou génétiques, de données de localisation, d'une adresse IP ou d'un autre identifiant, qui renvoient à une personne donnée ou à un dispositif ou un ensemble de dispositifs (ordinateur, téléphone portable, appareil photo, console de jeu, etc.). L'utilisation d'un pseudonyme ou de tout identifiant/identité numérique n'entraîne pas l'anonymisation des données, la personne concernée pouvant encore être identifiable ou individualisée. Les données pseudonymisées doivent donc être considérées comme des données à caractère personnel et sont à ce titre couvertes par les dispositions de la Convention.

17. Les données ne peuvent être considérées comme anonymes que lorsque la ré-identification de la personne concernée est impossible ou nécessiterait des délais, activités ou moyens déraisonnables. Des données en apparence anonymes car non assorties d'un élément d'identification évident peuvent néanmoins, dans certains cas (ne nécessitant pas des délais, activités ou moyens déraisonnables) permettre l'identification de la personne à laquelle elles sont associées. C'est notamment le cas lorsque, prises ensemble, des données physiques, physiologiques, génétiques, mentales, économiques,

[18] Voir Commissaire aux droits de l'homme du Conseil de l'Europe, « La prééminence du droit sur l'internet et dans le monde numérique en général », Document thématique, CommDH/IssuePaper(2014)1, 8 décembre 2014, p. 48, point 3.3 « Toute personne », sans discrimination.

culturelles ou sociales (comme l'âge, le sexe, l'activité professionnelle, la géolocalisation, la situation de famille, etc.) permettent au responsable du traitement ou à toute autre personne d'identifier la personne concernée. Dans pareille situation, les données ne sauraient être considérées comme anonymes et sont couvertes par les dispositions de la Convention.

18. Lorsque des données sont rendues anonymes, des moyens doivent être mis en place pour empêcher toute ré-identification des personnes concernées ; en particulier, tous les moyens techniques doivent être mis en œuvre pour garantir que la personne n'est pas ou plus identifiable. Vu la rapidité des évolutions techniques, l'anonymat des données devra être réévalué régulièrement.

19. La notion de « personne concernée » exprime également l'idée que la personne possède un droit subjectif par rapport aux données qui la concernent (le terme anglais est « data subject »), même lorsque le traitement de celles-ci est effectué par un tiers.

20. Si la Convention s'applique en principe au traitement de données relatives à des personnes vivantes, les Parties peuvent en étendre la protection aux personnes physiques décédées et aux personnes morales (cf. n° 33)

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

21. L'expression « traitement de données » recouvre une notion générale susceptible d'une interprétation flexible. Partant de la collecte ou création de données à caractère personnel, elle englobe toutes les opérations automatisées, qu'elles le soient totalement ou en partie. On parle aussi de traitement des données lorsqu'aucune opération automatisée n'est effectuée mais que les données sont organisées selon une structure qui permet au responsable du traitement ou à toute autre personne de rechercher, combiner ou mettre en corrélation des données relatives à une personne.

Lettre c [/d] – « responsable du traitement »

22. « Responsable du traitement » désigne la personne ou l'organe qui dispose du pouvoir de décision à l'égard du traitement de données, que ce soit en vertu d'une désignation officielle ou de circonstances factuelles à apprécier au cas par cas. Il peut y avoir plusieurs responsables ou co-responsables du traitement (conjointement responsables d'un traitement ou en charge de différents aspects d'un traitement). Les critères suivants sont pertinents pour savoir si l'organe ou la personne en question peut être qualifié de responsable du traitement : il ou elle doit avoir droit de regard sur les motifs justifiant le traitement, les moyens et méthodes du traitement, le choix des données à traiter et les personnes autorisées à y accéder. Le responsable du traitement demeure responsable des données traitées quelle que soit leur localisation et indépendamment de la personne qui procède aux opérations de traitement. De ce point de vue, les personnes qui ne sont pas subordonnées au responsable du traitement et qui effectuent le traitement pour son compte, conformément à ses instructions, sont des sous-traitants.

23. Le pouvoir décisionnel du responsable du traitement peut tenir au fait que le traitement de données à caractère personnel est sa principale activité (une agence de publicité qui traite des données personnelle pour produire des publicités ciblées, par exemple) ou qu'il contribue à celle-ci (création d'une base de données clients ou employés, traitement de données de clients pour l'exécution d'un contrat, etc.).

24. Aux termes de l'article 7bis sur la transparence du traitement, l'identité et la résidence ou le lieu d'établissement habituels du responsable du traitement ou des co-responsables du traitement le cas échéant, sont à fournir aux personnes concernées.

Lettre d [/e] – « destinataire »

25. « Destinataire » désigne la personne ou l'entité qui reçoit des données à caractère personnel ou à qui ces données sont rendues accessibles. Il peut être interne (service au sein de l'entité du responsable du traitement) ou externe (tierce partie). Selon le cas, le destinataire peut être un responsable du traitement, un sous-traitant ou la personne concernée elle-même. Par exemple, une entreprise peut envoyer les données de ses employés au ministère compétent, qui les traitera à des fins fiscales en tant que responsable du traitement. Elle peut les envoyer à une société proposant des services de stockage, celle-ci jouant alors le rôle de sous-traitant. Elle peut en donner une copie aux personnes concernées pour des raisons de transparence ou de vérification de la qualité. Le destinataire peut être un organisme public mais lorsque les données reçues par lui sont traitées dans le cadre d'une demande particulière conformément au droit applicable, il ne sera pas considéré comme un destinataire.

Lettre e [/f] – « sous-traitant »

26. Le « sous-traitant » est toute personne (autre que les employés du responsable du traitement) qui accomplit les opérations de traitement pour le compte et les besoins du responsable du traitement conformément à ses instructions, lesquelles définissent les limites de l'utilisation autorisée des données à caractère personnel par le sous-traitant. Si le sous-traitant ne respecte pas ces instructions, il traite les données illégalement.

Article 3 – Champ d'application

27. Conformément au paragraphe 1, les Parties s'engagent à appliquer la Convention à tout traitement de données relevant de leur juridiction, dans le secteur public comme dans le secteur privé. La notion de « juridiction » s'entend au sens de compétences traditionnelles de l'Etat, qu'il exerce en principe sur son territoire, à savoir les compétences normatives, juridictionnelles et d'exécution[19]. Tout traitement de données effectué par un établissement public relève directement de la juridiction de la Partie concernée, étant le produit de l'exercice de ses compétences. Les traitements de données effectuées 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, lorsque les activités impliquant le traitement des données sont réalisées sur ce territoire ou reliées au suivi du comportement de la personne concernée sur ce territoire, ou encore lorsque les activités de traitement sont liées à l'offre de services ou de biens à la personne concernée, sur ce territoire. La Convention est applicable lorsque les opérations de traitement des données relèvent de la juridiction de la Partie concernée, que ce soit dans le secteur public ou privé.

28. Le but visé en reliant le champ de la protection à la notion de « juridiction » des Parties est de mieux résister à l'épreuve du temps et aux progrès technologiques constants, ainsi qu'à l'évolution du concept juridique de « juridiction de l'Etat » en droit international[20], tout en renforçant l'engagement en faveur de la protection des personnes physiques.

[19] Voir Commissaire aux droits de l'homme du Conseil de l'Europe, « La prééminence du droit sur l'internet et dans le monde numérique en général », Document thématique, CommDH/IssuePaper(2014)1, 8 décembre 2014, p. 50-54, en particulier point 3.4. « [Se trouvant sur le territoire d'un Etat partie et] relevant de [sa] juridiction » : « Tout Etat qui utilise ses pouvoirs législatif et répressif pour s'emparer de données qui ne sont pas détenues sur son territoire physique, mais sur le territoire d'un autre Etat, en vue d'exercer un contrôle sur ces données – en général en exploitant l'infrastructure matérielle de l'internet et les systèmes de communication mondiale pour extraire ces données de serveurs situés dans l'autre Etat, ou en chargeant des organismes privés ayant accès à ces données à l'étranger de les extraire de serveurs situés dans un autre pays et de les remettre à l'Etat intéressé – exerce sa compétence de manière extraterritoriale au sein de la juridiction de l'autre Etat […] ».

[20] Voir notamment Cour européenne des droits de l'homme, *Issa et autres c. Turquie*, n° 31821/96, 16 novembre 2004, par. 66-71, et en particulier 68 « la notion de « juridiction » au sens de l'article 1 de la Convention ne se circonscrit pas nécessairement au territoire national des Hautes Parties contractantes […]. Dans des circonstances exceptionnelles, les actes des Etats contractants accomplis ou produisant des effets en dehors de leur territoire (« actes extraterritoriaux ») peuvent s'analyser en l'exercice par eux de leur juridiction au sens de l'article 1 de la Convention. ».

29. *Le paragraphe 1bis* exclut du champ de la Convention les traitements de données effectués dans le cadre d'activités [exclusivement] personnelles ou domestiques. Cela évite d'imposer des obligations déraisonnables à des traitements de données effectués par des personnes physiques dans la sphère personnelle, pour des activités liées à l'exercice de leur vie privée. On entend par « activités personnelles ou domestiques » des activités étroitement et objectivement liées à la vie privée d'une personne qui n'ont pas d'impact significatif sur la sphère personnelle d'autrui. Elles n'ont aucun aspect professionnel ou commercial et correspondent exclusivement à des activités personnelles ou domestiques comme le stockage de photos de famille ou de photos privées sur un ordinateur, la création d'une liste comportant les coordonnées d'amis ou de membres de la famille, la correspondance, etc. La notion de « sphère privée » renvoie notamment à la famille, à un cercle restreint d'amis ou à un cercle limité en taille, basé sur une relation personnelle ou une relation de confiance particulière.

30. Une activité sera « exclusivement personnelle ou domestique » suivant les circonstances. A titre d'exemple, lorsque des données personnelles sont rendues accessibles à un grand nombre de personnes ou à des personnes manifestement étrangères à la sphère privée, par exemple sur un site web public, l'exemption n'est pas applicable. De même, l'exploitation d'un système de caméra, donnant lieu à un enregistrement vidéo des personnes stocké dans un dispositif d'enregistrement continu tel qu'un disque dur, installé par une personne physique sur sa maison familiale afin de protéger les biens, la santé et la vie des propriétaires de la maison, mais qui s'étend, même partiellement, à l'espace public et, de ce fait, est dirigée vers l'extérieur de la sphère privée de celui qui procède au traitement des données par ce moyen, ne saurait être considérée comme une activité [exclusivement] « personnelle ou domestique »[21].

31. La Convention s'applique néanmoins aux traitements de données effectués par les fournisseurs des moyens de traitement de données à caractère personnel destinés à de telles activités personnelles ou domestiques. [La Convention s'applique néanmoins aux traitements de données effectués par les fournisseurs des services ou produits utilisés dans le cadre d'activités personnelles ou domestiques]. .

32. La Convention ne concerne que le traitement des données relatives à des personnes physiques mais les Parties peuvent prévoir dans leur droit interne une extension de la protection aux données relatives aux personnes morales afin de protéger les intérêts légitimes de celles-ci. La Convention s'applique aux personnes vivantes : elle n'a pas vocation à être appliquée aux données des personnes décédées. Cela n'empêche pas les Parties d'étendre la protection aux personnes décédées (par exemple pour répondre aux besoins croissants de protection de la réputation ou des intérêts de la personne décédée et/ou de ses héritiers).

Chapitre II – Principes de base pour la protection des données à caractère personnel

Article 4 – Engagements des Parties

33. Comme l'indique cet article, la Convention oblige les Parties à incorporer dans leur « loi » des dispositions sur la protection des données. Selon le système juridique concerné, la Convention peut être directement applicable, ce qui signifie que les droits des individus peuvent être exercés directement, indépendamment de toute mise en œuvre préalable dans le droit de la Partie en question.

34. L'expression « loi » des Parties désigne, suivant le système juridique et constitutionnel du pays considéré, toutes les règles ayant force exécutoire, qu'elles soient d'origine législative ou découlent de la jurisprudence. Ces règles doivent répondent aux exigences qualitatives d'accessibilité et de prévisibilité. Autrement dit, la loi doit être suffisamment claire pour permettre aux personnes physiques et autres entités de régler leur conduite à la lumière des conséquences juridiques prévisibles de leurs actes, et

---

Voir également la fiche thématique de la Cour européenne des droits de l'homme sur la juridiction extraterritoriale des Etats parties à la Convention européenne des droits de l'homme, décembre 2013, à l'adresse http://www.echr.coe.int/Documents/FS_Extra-territorial_jurisdiction_FRA.pdf.

[21] Voir Cour de Justice de l'UE, 11 décembre 2014, (Frantisek) C-212/13

toute personne susceptible d'être concernée par cette loi doit y avoir accès. L'expression englobe toutes les mesures, y compris les mesures organisationnelles ou instruments à adopter pour mettre en œuvre la Convention, applicables à un nombre illimité de cas et à un nombre indéterminé de personnes. Elle inclut 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. Elle couvre en particulier les Constitutions des Etats et tout acte écrit des autorités législatives (les lois au sens formel du terme) ainsi que toutes les mesures de réglementation (décrets, règlements, ordonnances et directives administratives) fondées sur ces lois, mais aussi les conventions internationales applicables en droit interne, y compris le droit de l'Union européenne. Le terme englobe 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, la jurisprudence constante relative à l'interprétation du droit écrit. Il concerne enfin tout acte d'un organisme professionnel exerçant des pouvoirs délégués par le législateur, conformément à ses pouvoirs de réglementation indépendants.

35. Ces mesures contraignantes peuvent être complétées utilement par des mesures de réglementation volontaire dans le domaine de la protection des données, par exemple des codes de bonnes pratiques ou des règles de conduite professionnelle. Cela dit, de telles mesures volontaires ne suffisent pas à elles seules pour assurer le respect plein et entier de la Convention.

36. S'agissant des organisations internationales[22], l'expression s'entend du droit interne de ces organisations, qui peut dans certains cas avoir un effet direct, au niveau national, dans chacun des Etats membres.

37. L'efficacité de l'application des mesures prises pour donner effet aux dispositions de la Convention revêt une importance fondamentale. Au-delà des dispositions législatives concrètes, le rôle de la ou des autorités de contrôle et l'ensemble des voies de recours mises à la disposition des personnes concernées devraient être pris en considération dans l'appréciation globale de l'efficacité de la mise en œuvre, par une Partie, des dispositions de la Convention.

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

39. Les Parties s'engagent, au paragraphe 3 de l'article 4, à contribuer activement au processus d'évaluation du respect de leurs engagements en vue de permettre une évaluation régulière de la mise en œuvre des principes de la Convention (et notamment de son efficacité). La présentation régulière de rapports sur l'application de la législation en matière de protection des données pourrait être un élément de cette contribution active des Parties.

40. L'évaluation de la conformité sera effectuée par le comité conventionnel selon une procédure objective, équitable et transparente établie par lui-même et décrite en détail dans son règlement.

Article 5 – Légitimité du traitement des données et qualité des données

[22] 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).

41. Le paragraphe 1 dispose que le traitement des données doit être proportionné, c'est-à-dire pertinent au regard du but légitime poursuivi, et nécessaire dans le sens où ce but ne peut être poursuivi par d'autres moyens appropriés moins attentatoires aux intérêts, droits et libertés des personnes concernées ou de la société dans son ensemble. Il ne doit pas induire une ingérence disproportionnée dans 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, y compris au stade initial, c'est-à-dire lorsqu'il est décidé de procéder ou non au traitement des données.

42. Le paragraphe 2 prévoit que la légalité du traitement de données est subordonnée à l'une ou l'autre des deux conditions essentielles que sont le consentement de la personne concernée ou l'existence de fondements légitimes prévus par la loi. Les paragraphes 1, 2 et 3 de l'article 5 sont cumulatifs et doivent être respectés pour garantir la légitimité du traitement des données.

43. Le consentement de la personne concernée doit être libre, spécifique, éclairé et [non équivoque]. Le consentement représente une déclaration de l'intention de la personne : c'est la libre expression d'un choix intentionnel, faite soit par le biais d'une déclaration (qui peut être écrite, y compris par des moyens électroniques, ou orale) soit par une action affirmative explicite qui indique clairement dans ce contexte spécifique l'acceptation du traitement des données à caractère personnel proposé. Par conséquent, le silence, l'inaction ou des formulaires ou cases à cocher prévalidés ne peuvent constituer un consentement. Le consentement doit couvrir l'ensemble des activités de traitement de données qui poursuivent la ou les mêmes finalités (lorsque les finalités sont multiples, un consentement doit être donné pour chacune d'entre elles). Il peut dans certains cas y avoir plusieurs décisions de consentement (lorsque la finalité est la même mais que les données sont de nature différente, par exemple des données de santé et des données de localisation : dans pareil cas, la personne concernée peut donner son consentement au traitement de ses données de localisation mais pas de ses données de santé). La personne concernée doit être pleinement consciente des implications de sa décision (ce que signifie le fait de donner son consentement et l'étendue de ce dernier) et donc avoir été dûment informée. Aucune influence ou pression (de nature économique ou autre), directe ou indirecte, ne peut être exercée sur la personne concernée et le consentement ne doit pas être considéré comme libre si elle n'a pas de véritable choix ou de liberté de choix ou ne peut refuser ou retirer son consentement sans préjudice (par exemple une augmentation du prix d'un service lorsqu'elle refuse le traitement de données à caractère personnel non nécessaires pour l'exécution d'un contrat).

44. L'expression d'un consentement ne dispense pas de respecter les principes fondamentaux de la protection des données à caractère personnel énoncés au chapitre II de la Convention : la proportionnalité du traitement, par exemple, doit toujours être évaluée.

45. La personne concernée est en droit de retirer son consentement à tout moment (ceci est à distinguer du droit de s'opposer à un traitement de données). Cela n'aura pas d'incidence sur la légalité du traitement des données effectué avant le retrait du consentement mais n'autorise plus aucun traitement des données, sauf si une autre base juridique le justifie.

46. La notion de « fondement légitime prévu par la loi » au paragraphe 2 englobe le traitement de données nécessaire à l'exécution d'un contrat (ou de mesures précontractuelles, à la demande de la personne concernée) auquel la personne concernée est partie ou à la protection d'intérêts vitaux de la personne concernée, ainsi que le traitement de données réalisé pour des motifs d'intérêt public ou pour des intérêts légitimes prédominants du responsable du traitement.

47. Le traitement de données pour des motifs d'intérêt public doit être prévu par la loi, notamment lorsqu'il s'agit d'un traitement à des fins monétaires, budgétaires et fiscales, de santé publique et de sécurité sociale, de prévention, d'investigation, de détection et de répression des infractions pénales et d'exécution des sanctions pénales, de protection de la sécurité nationale, de prévention, d'investigation, de détection et de répression des violations de la déontologie en ce qui concerne les professions réglementées, d'exécution des décisions civiles et de protection de l'indépendance de la magistrature et

de la procédure judiciaire. Un traitement de données peut servir à la fois un motif d'intérêt public et les intérêts vitaux des personnes concernées, par exemple dans le cas de données traitées à des fins humanitaires, notamment pour la surveillance d'une épidémie potentiellement mortelle et de sa propagation, ou dans le cas d'urgences humanitaires. Cette dernière éventualité peut se présenter dans des situations de catastrophes naturelles où le traitement des données à caractère personnel de personnes portées disparues peut se révéler nécessaire, pendant une durée limitée, à des fins liées au contexte d'urgence à évaluer au cas par cas. Cela peut également se produire dans des situations de conflit armé ou d'autres formes de violence[23].

48. Les conditions d'un traitement légitime sont énoncées aux paragraphes 3 et 4. Les données sont traitées licitement, loyalement et de manière transparente, et satisfont à des critères garantissant leur qualité. Elles doivent avoir été collectées pour des finalités explicites, déterminées et légitimes, et leur traitement doit être effectué pour ces finalités, ou du moins ne pas être incompatible avec celles-ci. La référence à des « finalités déterminées » indique qu'il n'est pas permis de traiter des données pour des finalités non définies, imprécises ou vagues. La légitimité d'une finalité dépendra des circonstances, le but étant de garantir dans chaque cas un juste équilibre entre 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. Un juste équilibre doit ainsi être ménagé entre les intérêts de la personne concernée et ceux du responsable du traitement ou de la société. Dans tous les cas, un traitement de données au service d'une intention illicite ne peut être considéré comme reposant sur une finalité légitime.

49. La notion d'utilisation « compatible » doit être interprétée de façon restrictive, pour 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 traitement ultérieur que la personne concernée pourrait considérer comme inattendu, inapproprié ou contestable.

50. Le traitement ultérieur des données à caractère personnel à des fins statistiques, historiques et scientifiques, dont il est question au paragraphe 4(b), est a priori jugé compatible à condition que des garanties complémentaires s'appliquent (par exemple, l'anonymisation ou la pseudonymisation des données sauf s'il est absolument indispensable de conserver la forme identifiable, des règles en matière de secret professionnel, des dispositions régissant l'accès restreint et la diffusion restreinte de données aux fins précitées, notamment celles liées aux statistiques et à l'archivage public, ainsi que d'autres mesures d'ordre technique et organisationnel visant la sécurité des données) et que les opérations, par définition, excluent toute utilisation de l'information obtenue pour la prise de décisions ou de mesures concernant une personne donnée. L'expression « *fins statistiques* » se réfère aux enquêtes statistiques ou à la production de résultats statistiques. Les statistiques visent à analyser et à caractériser des phénomènes collectifs ou de masse dans une population donnée[24]. Le secteur public et le secteur privé peuvent poursuivre des fins statistiques. Le traitement de données *« à des fins scientifiques »* vise à fournir à la recherche une information qui contribue à la compréhension de phénomènes dans divers domaines scientifiques (épidémiologie, psychologie, économie, sociologie, linguistique, politologie, criminologie, etc.) en vue d'établir des permanences, des lois de comportement ou des schémas de causalité qui transcendent tous les individus qu'ils concernent[25]. Les fins « *historiques »* incluent l'archivage dans l'intérêt public et la recherche généalogique.

[23] Auquel cas les textes applicables sont les quatre conventions de Genève de 1949 et leurs protocoles additionnels de 1977 ainsi que les Statuts du mouvement international de la Croix-Rouge et du Croissant-Rouge.

[24] Recommandation n° R (97) 18 du Comité des Ministres aux Etats membres concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques, 30 septembre 1997, annexe, point 1.

[25] Exposé des motifs de la Recommandation n° R (97) 18 du Comité des Ministres aux Etats membres concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques, 30 septembre 1997, paragraphes 11 et 14.

51. Les données personnelles faisant l'objet d'un traitement doivent être adéquates, pertinentes et non excessives. Elles doivent en outre être exactes et, le cas échéant, mises à jour régulièrement.

52. La règle figurant au paragraphe 4(c) selon laquelle les données faisant l'objet d'un traitement ne doivent pas être excessives exige en premier lieu que les données soient limitées au strict minimum nécessaire par rapport aux finalités pour lesquelles elles sont traitées. Elles ne seront traitées que dans la mesure où ces finalités ne peuvent être atteintes en utilisant des informations ne comportant pas de données à caractère personnel. Cette disposition vise aussi bien les aspects quantitatifs que qualitatifs des données à caractère personnel. Des données qui seraient adéquates et pertinentes mais entraîneraient une ingérence disproportionnée dans les droits et libertés fondamentaux en jeu doivent être considérées comme excessives et ne pas être traitées. Tel serait le cas, par exemple, dans une procédure de recrutement pour un poste administratif classique où la collecte, par l'employeur potentiel, de données sur la sérologie VIH des candidats pourrait être considérée comme un traitement de données pertinentes (en vue de la gestion des absences futures, par exemple) mais se révèle excessive car elle implique une ingérence disproportionnée dans le droit au respect de la vie privée du candidat par rapport à l'intérêt que présentent ces données pour l'employeur potentiel.

53. L'exigence relative à la durée de conservation limitée des données à caractère personne, figurant au paragraphe 4(e), signifie que les données doivent être effacées une fois que la finalité pour laquelle elles ont été collectées a été atteinte, ou être conservées sous une forme empêchant toute identification directe ou indirecte de la personne concernée.

Article 6 – Catégories particulières de données

54. Le traitement de certaines catégories de données ou le traitement de données pour les informations sensibles qu'elles révèlent, peut conduire à empiéter sur certains intérêts, droits et libertés. Tel est le cas par exemple lorsqu'il existe un risque potentiel de discrimination ou d'atteinte à la dignité ou à l'intégrité physique d'une personne, lorsque la sphère la plus intime de la personne concernée, par exemple sa vie sexuelle ou son orientation sexuelle, est visée ou encore lorsque le traitement des données risque de porter atteinte à la présomption d'innocence. Ce traitement n'est autorisé que si la loi prévoit une protection renforcée par des garanties appropriées qui complètent les autres dispositions protectrices de la Convention. .

55. Afin d'éviter tout effet préjudiciable pour la personne concernée, le traitement de données sensibles à des fins légitimes doit être assorti de garanties appropriées (adaptées aux risques 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 ou indiquant les cas exceptionnels dans lesquels le traitement de ces données serait autorisé, le secret professionnel, des mesures faisant suite à une analyse de risque, ou une mesure de sécurité particulière d'ordre organisationnel ou technique (chiffrement des données, par exemple).

56. 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 sur sa santé ou sa filiation, et celles de tiers. Les données génétiques sont toutes les données relatives aux caractéristiques héréditaires d'un individu ou acquises à un stade précoce du développement prénatal, résultant de l'analyse d'un échantillon biologique de cet individu : analyse des chromosomes, de l'ADN ou de l'ARN ou de tout autre élément permettant d'obtenir des informations équivalentes. Des risques analogues sont posés par le traitement de données concernant des infractions pénales (y compris présumées), des condamnations pénales (reposant sur le droit pénal et dans le cadre d'une procédure pénale) et les mesures de sécurité connexes (notamment la privation de liberté), nécessitant des garanties appropriées pour les droits et libertés des personnes concernées.

57. Le traitement de données biométriques, c'est-à-dire de données résultant d'un traitement technique spécifique de données relatives aux caractéristiques physiques, biologiques ou physiologiques d'un individu qui permet l'identification unique de ce dernier, est également considéré comme ayant un caractère sensible lorsqu'il est précisément utilisé pour identifier de façon unique la personne concernée.

58. Le traitement de photographies ne sera pas systématiquement considéré comme un traitement de données sensibles, les photographies n'étant couvertes par la définition des données biométriques que lorsqu'elles sont traitées par un moyen technique spécifique permettant l'identification ou l'authentification uniques d'un individu. Par ailleurs, lorsque le traitement d'images vise à révéler des informations sur l'origine raciale ou la santé d'une personne (voir point suivant), il sera considéré comme un traitement de données sensibles. Au contraire, le traitement d'images par un système de vidéosurveillance pour des raisons de sécurité dans une zone commerciale ne sera pas considéré comme tel.

59. Le traitement de données sensibles risque de porter atteinte aux droits des personnes concernées lorsqu'il est réalisé pour les informations spécifiques qu'elles révèlent. Ainsi, le traitement des noms de famille, qui dans bien des cas ne présente aucun risque pour les individus (par exemple pour l'établissement courant de bulletins de salaire), pourrait impliquer des données sensibles, par exemple s'il a pour finalité de révéler l'origine ethnique ou les convictions religieuses de personnes à partir de l'origine linguistique de leur nom. Le traitement de données en vue d'obtenir des informations sur la santé englobe le traitement d'informations concernant la santé physique ou mentale passée, actuelle et future d'un individu, lequel peut être malade ou bien portant. Le traitement de photographies de personnes qui portent des lunettes, ont une jambe cassée ou présentent des brûlures ou toute autre caractéristique visible liée à la santé ne sera pas considéré comme un traitement de données sensibles si les données de santé ne sont pas extraites des images et ne sont pas traitées en tant que telles.

60. Lorsque des données sensibles doivent être traitées à des fins statistiques (par exemple pour disposer de statistiques en matière d'égalité ou pour obtenir des informations sur la santé de la population), elles devraient être collectées de manière à ce que la personne concernée ne soit pas identifiable. La collecte de données sensibles sans données d'identification est une garantie au sens de l'article 6 de la Convention. Lorsqu'il existe un besoin légitime de collecter des données sensibles à des fins statistiques sous une forme identifiable (de manière à pouvoir réaliser des enquêtes répétées, par exemple), des garanties appropriées doivent être mises en place : des mesures pour séparer les données sensibles des données d'identification dès la collecte sauf si cela n'est pas faisable, l'obtention du consentement explicite de la personne concernée avant l'étude (le simple fait de fournir des données ne peut être considéré comme un consentement) sauf si un motif d'intérêt public important justifie une dérogation à cette obligation, ainsi que l'interdiction de publication et de diffusion des données à caractère personnel[26].

Article 7 – Sécurité des données

61. Le responsable du traitement ou, le cas échéant, le sous-traitant, prend des mesures de sécurité spécifiques d'ordre technique et organisationnel pour chaque traitement, en tenant compte des effets dommageables potentiels pour l'individu, de la nature des données à caractère personnel, du volume de données à caractère personnel traitées, 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'une conservation à long terme, etc.

62. Les mesures de sécurité doivent reposer sur les méthodes et techniques de pointe en matière de sécurité des données dans le cadre du traitement de données. 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.

[26] Voir la Recommandation n° R (97) 18 du Comité des Ministres aux Etats membres concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques, 30 septembre 1997.

63. Les mesures de sécurité visent à prévenir de nombreux risques. Cela dit, le paragraphe 2 contient une obligation spécifique rétroactive au cas où il y aurait néanmoins une violation des données susceptible de porter gravement atteinte aux droits et libertés fondamentaux de la personne concernée. Par exemple, la révélation de données couvertes par le secret professionnel, susceptible d'entraîner un préjudice financier, une atteinte à la réputation, des dommages corporels ou une humiliation, pourrait être jugée constitutive d'une atteinte « grave ».
64. En cas de violation de données à caractère personnel, le responsable du traitement est tenu de notifier l'incident aux autorités de contrôle compétentes. C'est l'exigence minimale. Il doit également informer l'autorité de contrôle de toute mesure prise ou proposée pour remédier à la violation et pallier les conséquences potentielles.

65. Le fait d'avoir signalé l'incident aux autorités de contrôle n'empêche pas le responsable du traitement de procéder à des notifications complémentaires. Il devrait par exemple être encouragé à informer les personnes concernées, notamment lorsque la violation des données est de nature à engendrer un risque important pour leurs droits et libertés, par exemple un traitement discriminatoire, un vol ou une usurpation d'identité, des pertes financières, une atteinte à la réputation, une perte de confidentialité des données protégées par le secret professionnel ou tout autre préjudice économique ou social lourd, et leur fournir des renseignements adéquats et utiles afin qu'elles sachent où s'adresser et quelles mesures prendre pour atténuer les effets néfastes de la violation des données. Si le responsable du traitement n'informe pas spontanément la personne concernée de la violation des données, l'autorité de contrôle, après examen des effets négatifs potentiels de celle-ci, devrait être autorisée à demander au responsable du traitement de le faire. Une notification à d'autres autorités compétentes, par exemple celles chargées de la sécurité des systèmes informatiques, peut également être exigée.

Article 7bis – Transparence du traitement

66. Le responsable du traitement doit faire preuve de transparence dans la conduite des opérations afin de garantir un traitement loyal et de permettre aux personnes concernées de comprendre et partant, d'exercer pleinement leurs droits dans le cadre du traitement considéré.

67. Le responsable du traitement doit fournir un minimum d'informations aux personnes concernées lorsqu'il collecte leurs données, directement ou indirectement (pas par leur intermédiaire). Les exigences de transparence sont obligatoires mais les informations sur le nom et l'adresse du responsable, la base légale et les finalités du traitement effectué, les catégories de données traitées et leurs destinataires (évidents ou non) ainsi que les moyens d'exercer les droits, peuvent être fournies sous tout format approprié (par le biais d'un site web, d'outils technologiques sur des dispositifs personnels, etc.) dans la mesure où elles sont présentées de manière effective et loyale à la personne concernée. Ces informations doivent être facilement accessibles, lisibles, compréhensibles et adaptées aux personnes concernées (dans un langage adapté aux enfants, par exemple). Tout autre renseignement nécessaire pour garantir un traitement loyal des données, comme la durée de conservation des données, le raisonnement qui sous-tend le traitement des données ou des informations sur les transferts de données vers un pays étranger (notamment sur la question de savoir si ce pays offre ou non un niveau de protection approprié et sur les mesures prises par le responsable du traitement pour garantir un tel niveau de protection) devra également être fourni.

68. Le responsable du traitement n'est pas tenu de fournir ces informations lorsque la personne concernée les a déjà reçues et qu'il est en mesure de le prouver, ou dans le cas d'une collecte indirecte de données par le biais de tiers lorsque cette éventualité est expressément prévue par la loi (qui doit être précise et suffisamment détaillée), ou lorsque cela lui est impossible ou impliquerait des efforts disproportionnés parce que la personne concernée n'est pas directement identifiable ou qu'il n'a aucun moyen de la contacter. Cette impossibilité peut être d'ordre juridique (dans le cadre d'une enquête pénale ou lorsque les personnes qui détiennent les informations nécessaires sont tenues au secret professionnel, par exemple) ou pratique (par exemple lorsqu'un responsable du traitement ne traite que des images et ignore le nom et les coordonnées des personnes concernées).

69. Lorsqu'une telle impossibilité est d'ordre pratique, le responsable du traitement doit néanmoins utiliser tous les moyens disponibles, raisonnables et économiquement abordables pour informer les personnes concernées, d'une manière générale ou individuellement. Cela peut être fait à un stade ultérieur, par exemple lorsque le responsable du traitement est mis en contact avec la personne concernée pour une raison quelconque.

Article 8 – Droits des personnes concernées

70. Les dispositions énoncées dans cet article établissent la liste des droits que chaque personne doit être en mesure d'exercer et de défendre relativement au traitement de données à caractère personnel la concernant.

71. Ces droits se composent des principaux éléments suivants, qui constituent des outils essentiels pour la personne concernée :
– le droit de ne pas être soumise à une décision purement automatisées sans que son point de vue n'ait été pris en considération (lettre a) ;
– le droit d'être informée de l'existence d'un traitement la concernant et d'accéder aux données (lettre b) ;
– le droit d'être informée du raisonnement qui sous-tend le traitement de données (lettre c) ;
– le droit de s'opposer à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement (lettre d) ;
– le droit de rectification ou d'effacement de données inexactes, erronées, ou d'une manière générale, de données dont le traitement est illicite (lettre e) ;
– le droit de disposer d'un recours si l'un quelconque des droits précités n'est pas respecté (lettre f) ;
– le droit de bénéficier de l'assistance d'une autorité de contrôle (lettre g).

72. Ces droits doivent être conciliés avec d'autres droits et intérêts légitimes. Conformément à l'article 9, ils ne peuvent faire l'objet d'autres restrictions que celles qui constituent des mesures nécessaires et proportionnées 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, dont des « secrets protégés par la loi » (secrets commerciaux, par exemple).

73. 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, il s'agit du responsable du traitement des données ou du sous-traitant qui l'exécute pour son compte. Néanmoins, dans des circonstances exceptionnelles énoncées à l'article 9 (sécurité nationale, par exemple), les droits d'accès, de rectification et d'effacement peuvent être exercés par l'intermédiaire de l'autorité de contrôle. S'agissant de données relatives à la santé, les droits peuvent également être exercés autrement que par un accès direct, par exemple avec l'assistance d'un professionnel de santé lorsque cela est dans l'intérêt de la personne concernée, notamment pour l'aider à comprendre les données ou faire en sorte que son état psychologique soit dûment pris en compte lors de la communication de l'information, toujours dans le respect des principes déontologiques.

74. *Lettre a.* Il est essentiel que toute personne susceptible d'être soumise à une décision purement automatisée ait le droit de contester cette décision en faisant valoir de manière effective son point de vue et ses arguments. En particulier, la personne concernée doit avoir la possibilité de prouver l'inexactitude éventuelle des données à caractère personnel avant leur utilisation, l'inadéquation du profil qu'il est prévu d'appliquer à sa situation particulière ou d'autres facteurs qui auront un impact sur le résultat de la décision automatisée. Tel est notamment le cas lorsque l'application d'un raisonnement algorithmique a pour effet de stigmatiser des individus [comme étant potentiellement coupables de fraude fiscale ou sociale] [ou lorsque leur capacité d'emprunt est évaluée par un logiciel].

75. *Lettre b.* Les personnes concernées doivent avoir connaissance du traitement de leurs données à caractère personnel. Alors que le droit d'accès devrait en principe être gratuit, la lettre b est rédigée de

manière à permettre au responsable du traitement de demander des frais raisonnables lorsque les demandes sont excessives et vise à couvrir les différentes formules pouvant être adoptées par les Parties, selon le cas : communication gratuite des données à intervalles réguliers ou communication moyennant paiement d'une somme forfaitaire tenant compte du coût administratif réel d'une réponse à une demande. Ces frais devraient être exceptionnels et dans tous les cas raisonnables, et ne pas empêcher ou dissuader les personnes concernées d'exercer leurs droits. Le responsable du traitement peut également refuser de répondre à des demandes manifestement infondées ou excessives. 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.

76. *Lettre c.* Les personnes concernées ont le droit d'obtenir connaissance du raisonnement qui sous-tend le traitement de données (automatisé ou non), y compris les conséquences de ce raisonnement et les conclusions qui peuvent en avoir été tirées. Par exemple, dans le cas d'un système d'évaluation de leur solvabilité par notation, les emprunteurs ont le droit d'obtenir connaissance de la logique sur laquelle repose le traitement de leurs données et qui aboutit à la décision d'octroi ou de refus du crédit, au lieu d'être simplement informés de la décision elle-même. Sans compréhension de ces éléments, d'autres garanties essentielles comme le droit d'opposition et le droit de recours auprès de l'autorité compétente ne pourront être exercées de manière effective.

77. *Lettre d.* En ce qui concerne le droit d'opposition, le responsable du traitement peut avoir un motif légitime de traiter les données, qui prévaut sur les intérêts ou les droits et libertés de la personne concernée. La constatation, l'exercice ou la défense d'un droit en justice peuvent être considérés comme des motifs légitimes impérieux justifiant la poursuite du traitement des données. L'existence de tels motifs devra être démontrée au cas par cas et la poursuite du traitement en l'absence de preuves pourrait être considérée comme illicite.

78. L'opposition au traitement des données à des fins commerciales devrait en principe entraîner l'effacement ou la suppression, sans autre condition, des données à caractère personnel faisant l'objet de l'opposition.

79. Le droit d'opposition peut être limité par la loi, par exemple aux fins de l'investigation ou de la répression d'infractions pénales. Lorsque le traitement des données repose sur un consentement valablement donné par la personne concernée, le droit d'opposition s'accompagne du droit de retirer le consentement. Toute personne peut retirer son consentement si elle assume les conséquences pouvant découler d'autres textes juridiques, comme l'obligation de dédommager le responsable du traitement.

80. *Lettre e.* La rectification ou l'effacement, s'ils se justifient, doivent être gratuits. Lorsque des rectifications et effacements sont obtenus conformément au principe énoncé à la lettre e, ils doivent, dans la mesure du possible, être portés à la connaissance des destinataires de l'information originale, à moins que cela se révèle impossible ou implique des efforts disproportionnés.

81. *La lettre g* vise à assurer une protection effective des individus en leur donnant droit à l'assistance d'une autorité de contrôle dans l'exercice des droits prévus par la Convention. Lorsque la personne en question réside sur le territoire d'une autre Partie, elle doit avoir la possibilité de présenter sa demande par l'intermédiaire de l'autorité désignée par cette Partie. La demande d'assistance doit contenir tous les éléments nécessaires concernant notamment : le nom, l'adresse et tout autre élément pertinent d'identification de la personne à l'origine de la demande ; le traitement auquel la demande se réfère, ou le responsable du traitement ; l'objet 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 pour préserver les intérêts d'une procédure judiciaire en cours.

82. En outre, il est à noter que l'indication de la finalité du traitement, les conditions à remplir pour assurer sa légitimité, les exigences de qualité des données, le droit de rectification et d'effacement des données, ainsi que la disposition relative à la durée de conservation des données (article 5.4. *e*.), associés à un droit effectif d'opposition et de retrait du consentement, offrent un niveau de protection approprié aux

personnes concernées. Cet ensemble de droits et de critères correspond dans la pratique à l'effet de ce qu'il est convenu d'appeler le « droit à l'oubli ».

Article 8bis - Obligations complémentaires

83. Pour assurer un droit effectif à la protection des données à caractère personnel, des obligations complémentaires doivent être imposées au responsable du traitement ainsi que, le cas échéant, au(x) sous-traitant(s).

84. Conformément au *paragraphe 1*, l'obligation faite au responsable du traitement d'assurer une protection adéquate des données est liée à la responsabilité de vérifier et de démontrer que le traitement de données est conforme au droit en vigueur. 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 devront prendre des mesures appropriées comme la formation des employés, la mise en place de procédures appropriées de notification (indiquant par exemple quand des données doivent être effacées du système), l'établissement de clauses contractuelles particulières en cas de délégation du traitement, pour donner effet à la Convention, ainsi que la mise en place de procédures internes permettant la vérification et la démonstration de la conformité.

85. L'une des mesures qui pourraient être prises par le responsable du traitement pour faciliter la vérification et la démonstration de 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 au responsable du traitement et sa désignation devra être notifiée à l'autorité de contrôle.

86. *Le paragraphe 2* précise qu'avant d'effectuer un traitement, le responsable du traitement doit examiner son impact potentiel sur les droits et libertés fondamentales des personnes concernées. Cet examen peut être informel et n'implique pas nécessairement une évaluation complète et systématique des risques et des impacts en matière de protection des données. Il évaluera également le respect du principe de proportionnalité, en s'appuyant sur une présentation détaillée du traitement qui inclura la nature des données, la portée, le contexte et les finalités du traitement ainsi que la probabilité et la gravité des risques encourus pour les droits et libertés des individus. Dans certains cas, lorsqu'un sous-traitant intervient en plus du responsable du traitement, il peut également se voir imposer l'obligation de procéder à un examen des risques. L'existence d'une telle obligation sera déterminée en tenant compte de la présentation détaillée du traitement. L'assistance de développeurs de systèmes d'information (et notamment de spécialistes de la sécurité) ou de concepteurs ainsi que d'usagers et de juristes dans l'examen des risques serait utile et pourrait permettre de réduire la charge de travail liée à cet exercice.

87. Conformément au *paragraphe 3*, pour que l'existence d'un degré de protection approprié soit encore mieux garantie, les responsables du traitement et le cas échéant les sous-traitants, veillent à ce que les exigences en matière de protection des données soient intégrées dès que possible dans les opérations de traitement, c'est-à-dire dans l'idéal au stade de la conception du système et de l'architecture, par des mesures techniques et organisationnelles (protection des données dès la phase de conception). Cet objectif ne doit pas uniquement concerner la technologie employée pour le traitement, mais également les activités connexes et les processus de gestion. Des fonctionnalités simples d'utilisation et facilitant la conformité avec le droit en vigueur devraient être en place. Par exemple, un accès sécurisé aux données en ligne devrait être proposé aux personnes concernées, lorsque cela est possible et justifié. Il devrait également y avoir des outils faciles d'utilisation permettant aux personnes concernées de transférer leurs données à un autre fournisseur de leur choix ou de conserver elles-mêmes les données (outils de portabilité des données). Lors de la définition des exigences techniques de la configuration par défaut, les

responsables du traitement et les sous-traitants devraient choisir un paramétrage par défaut favorable au respect de la vie privée de manière à ce que l'utilisation des applications et logiciels ne porte pas atteinte au droit à la protection des données personnelles ; ils appliqueront notamment le principe de minimisation des données (protection des données par défaut). Par exemple, la configuration par défaut des réseaux sociaux devrait être telle que les messages ou les images ne soient partagés qu'avec un cercle restreint et choisi d'individus et non avec l'ensemble des internautes.

88. *Le paragraphe 4* autorise les Parties à moduler et adapter les obligations complémentaires prévues aux paragraphes 1 à 3 eu égard aux risques encourus pour les intérêts, les droits et les libertés fondamentales des personnes concernées. Une telle adaptation doit tenir compte de la nature et du volume des données traitées, de la nature, de la portée et de la finalité du traitement et, dans certains cas, de la taille de l'entité responsable du traitement. Ces obligations pourraient être modulées, par exemple, pour faire en sorte qu'elles n'entraînent pas de charges démesurées pour les petites et moyennes entreprises qui traitent uniquement des données à caractère personnel non sensibles reçues de consommateurs dans le cadre d'activités commerciales et ne les réutilisent pas ni ne les revendent à d'autres fins. Des dispenses de certaines obligations énoncées dans cet article pourront même être prévues pour certaines catégories de traitements, par exemple ceux ne présentant aucun risque pour les personnes physiques.

Article 9 – Exceptions et restrictions

89. Des exceptions aux principes de protection des données à caractère personnel sont autorisées de manière restrictive pour un nombre limité de dispositions, à condition qu'elles soient prévues par la loi et nécessaires, dans une société démocratique, aux motifs spécifiques dont la liste exhaustive est donnée aux lettres a et b de l'article 9, paragraphe 1. Une mesure « nécessaire dans une société démocratique » doit poursuivre un but légitime et donc 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 avancés par les autorités nationales pour le justifier doivent être pertinents et suffisants. Enfin, elle doit être établie par une loi accessible et prévisible, qui doit être suffisamment détaillée.

90. La nécessité de telles mesures doit être examinée au cas par cas, 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 ou de l'organisation internationale qui peuvent exiger des exceptions. Ces dernières ont été formulées de manière très précise pour éviter de donner aux Parties une marge de manœuvre trop importante dans l'application générale de la Convention.

91. La notion de « sécurité nationale » s'entend de manière restrictive, au sens de la protection de la souveraineté nationale de la Partie concernée contre des menaces internes ou externes, y compris la protection des relations internationales de la Partie, et doit être interprétée à la lumière de la jurisprudence pertinente de la Cour européenne des droits de l'homme qui inclut en particulier la protection de la sûreté de l'Etat et de la démocratie constitutionnelle contre l'espionnage, le terrorisme et le soutien au terrorisme et au séparatisme. Lorsque la sécurité nationale est en jeu, il doit exister des garanties pour éviter tout pouvoir discrétionnaire absolu[27]. Les mesures portant atteinte aux droits de l'homme doivent faire l'objet d'une forme de procédure contradictoire devant un organe indépendant et compétent pour examiner les motifs de la décision et les preuves pertinentes[28]. L'individu doit pouvoir contester l'affirmation de l'exécutif selon laquelle la sécurité nationale se trouve menacée[29]. Toute personne qui fait l'objet d'une

[27] Voir Division de recherche de la Cour européenne des droits de l'homme, « Sécurité nationale et jurisprudence européenne », novembre 2013, disponible à l'adresse http://www.coe.int/t/dghl/standardsetting/dataprotection/judgments_FR.asp

[28] Cour européenne des droits de l'homme, *Klass et autres c. Allemagne*, 6 septembre 1978, série A, n° 28 ; *Al-Nashif c. Bulgarie,* n° 50963/99, 20 juin 2002.

[29] Cour européenne des droits de l'homme, *Al-Nashif c. Bulgarie*, n° 50963/99, 20 juin 2002.

mesure basée sur des motifs de sécurité nationale doit bénéficier de garanties contre l'arbitraire[30]. La conservation d'informations dans les dossiers des services de la sûreté pendant une longue période doit se fonder sur des motifs pertinents et suffisants au regard de la protection de la sécurité nationale[31].

92. L'expression « intérêts économiques et financiers importants » 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, investigation et répression des infractions pénales » contenue dans cette lettre inclut les poursuites pénales.

93. *La lettre b* concerne les intérêts majeurs des parties privées, dont ceux de la personne concernée elle-même (par exemple lorsque ses intérêts vitaux sont menacés parce qu'elle est portée disparue) ou ceux d'autrui, tels que la liberté d'expression, y compris la liberté d'expression académique, artistique ou littéraire, le droit de communiquer des informations et d'en recevoir, la confidentialité de la correspondance et des communications, les secrets professionnels ou commerciaux ainsi que d'autres secrets protégés par la loi.

94. Le troisième paragraphe donne la possibilité de restreindre les droits pour certains traitements de données effectués à des fins historiques, statistiques ou scientifiques qui ne posent aucun risque identifiable pour la protection des données à caractère personnel, lorsque les restrictions aux droits de la personne concernée sont justifiées. Par exemple, l'utilisation de données pour des travaux statistiques, dans le domaine public comme dans le domaine privé, relève de cette hypothèse dans la mesure où ces données sont publiées sous une forme agrégée et dissociées de leurs identifiants, à condition que des garanties appropriées en matière de protection des données soient en place (voir paragraphe 51).

Article 10 – Sanctions et recours

95. Pour que la Convention garantisse un niveau approprié de protection des données, les obligations du responsable du traitement et du sous-traitant et les droits des personnes concernées doivent être assorties de sanctions et de recours dans la législation des Parties.

96. Il appartient à chacune des Parties de déterminer la nature (civile, administrative, pénale) de ces sanctions juridictionnelles et non juridictionnelles, Elles doivent être effectives, proportionnées et dissuasives. Il en va de même des voies de recours : les personnes concernées doivent avoir la possibilité de contester devant un tribunal une décision ou une pratique, selon des modalités dont la définition est laissée à l'appréciation des Parties. Des recours non juridictionnels doivent également être mis à la disposition des personnes concernées. Une indemnisation financière pour tous les dommages, y compris d'ordre moral, provoqués par le traitement des données, ainsi que des recours collectifs, peuvent également être envisagés.

Article 11 – Protection plus étendue

97. Cet article se fonde sur 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 disposées à adopter. Le texte souligne que ces principes ne constituent qu'une base à partir de laquelle les Parties pourront établir un système de protection plus développé.

Chapitre III – Flux transfrontières de données à caractère personnel

[30] Cour européenne des droits de l'homme, *Dalea c. France* (déc.), 964/07, 2 février 2010.
[31] Cour européenne des droits de l'homme, *Segerstedt-Wiberg et autres c. Suède*, n° 62332/00, CEDH 2006-VII.

Article 12 – Flux transfrontières de données à caractère personnel

98. Cet article a pour but de faciliter la libre circulation de l'information sans considération de frontières (rappelée dans le Préambule) tout en assurant une protection adéquate des personnes à l'égard du traitement des données à caractère personnel.

99. Le régime des flux transfrontières vise à garantir que des données à caractère personnel traitées à l'origine dans la juridiction d'une Partie (données collectées ou conservées dans cette juridiction, par exemple) puis soumises à la juridiction d'un Etat non partie à la Convention continuent d'être traitées conformément à des principes de protection des données appropriés au regard de la Convention. L'important est que les personnes concernées à l'origine par les données traitées dans la juridiction d'une Partie soient toujours protégées par des principes adéquats indépendamment de la loi applicable aux traitements considérés. Il existe une grande variété de régimes de protection possibles mais la protection doit être d'une qualité suffisante pour garantir que l'internationalisation du traitement des données et les flux transfrontières de données n'ont pas de conséquences négatives sur les droits de l'homme.

100. 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 organisation internationale.

101. L'article 12 ne s'applique qu'à l'exportation de données et non pas à leur importation, les données relevant alors du régime de protection des données de la Partie destinataire.

102. *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 relatifs à des Parties tenues de respecter des règles de protection harmonisées communes à des Etats appartenant à une organisation régionale. Tel est le cas des Etats membres de l'Union européenne. Ils sont liés par les règles adoptées à l'échelon de l'Union, qui s'appliquent aux flux transfrontières de données. Cette disposition vise à faire en sorte que tous les Etats contractants, ayant souscrit au « noyau dur » des dispositions de la Convention en matière de protection des données, offrent un niveau de protection jugé approprié. En l'absence d'autres règles régionales harmonisées et contraignantes régissant les flux de données, les flux de données à caractère personnel entre les Parties devraient avoir lieu librement.

103. Cela n'empêche pas une Partie de prendre certaines mesures pour s'informer de la circulation de données entre son territoire et celui d'une autre Partie, par exemple au moyen de déclarations à présenter par les responsables des traitements. Cependant, de telles mesures ne doivent pas être utilisées par une Partie comme moyen d'accéder aux données à caractère personnel des personnes relevant de sa juridiction.

104. Il peut arriver que des flux de données à caractère personnel partent simultanément d'une Partie vers plusieurs organisations internationales ou pays étrangers, dont certains sont Parties à la Convention et d'autres non. Dans ce cas, la Partie à l'origine du transfert de données, qui a des procédures d'exportation pour les Etats non parties, ne sera peut-être pas toujours en mesure d'éviter que ces procédures soient appliquées également aux données destinées à une autre Partie à la Convention ; en tout état de cause, elle devra procéder de façon à ce que les procédures en question ne soient pas un obstacle aux transferts de données vers celle-ci.

105. *Le paragraphe 2* réglemente les flux transfrontières de données à caractère personnel vers un destinataire qui ne relève pas de la juridiction d'une Partie. Comme pour tout flux de données à caractère personnel au-delà des frontières nationales, un niveau de protection approprié dans le pays 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 de garantir que le niveau de

protection des données est effectivement approprié : les règles de droit, d'une part, et des garanties ad hoc ou standardisées agréées, juridiquement contraignantes, opposables et dûment mises en œuvre, d'autre part.

106. Les *paragraphes 2 et 3* s'appliquent à toutes les formes de protection appropriée, qu'elles soient établies par des règles de droit ou des garanties standardisées. La loi doit inclure les éléments pertinents en matière de protection des données énoncés dans la présente Convention. Le niveau de protection devra être évalué au cas par cas et pour chaque transfert ou catégorie de transfert. Plusieurs éléments du transfert doivent être examinés et en particulier : la nature des données, les finalités et la durée des traitements pour lesquels les données sont transférées, le respect de la prééminence du droit par le 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 respectées.

107. Le contenu des garanties *ad hoc* ou standardisées doit inclure les éléments pertinents de la protection des données. En outre, les clauses contractuelles pourraient, par exemple, prévoir que la personne concernée dispose d'une personne de référence auprès du responsable du transfert qui soit chargée de veiller au respect des normes matérielles de protection. La personne concernée pourrait s'adresser à elle à tout moment et sans frais lié au traitement ou aux flux de données et, le cas échéant, obtenir son aide pour l'exercice de ses droits.

108. L'appréciation du niveau adéquat de protection doit prendre en considération les principes de la Convention et la manière dans laquelle ils sont respectés dans l'Etat ou l'organisation destinataires - dans la mesure où ils sont pertinents pour le cas spécifique de transfert - ainsi que la façon dont la personne concernée peut défendre ses intérêts en cas de non-conformité. L'évaluation doit également porter sur le caractère exécutoire des droits des personnes concernées et l'existence de recours juridictionnels et administratifs effectifs pour les personnes dont les données font l'objet d'un transfert. Une évaluation peut aussi être faite pour l'ensemble d'un Etat ou d'une organisation permettant ainsi tous les transferts de données vers cette destination. Le niveau adéquat de protection est déterminé par l'autorité de contrôle compétente de chaque Partie.

109. *Le paragraphe 4* permet aux Parties de déroger, dans des cas particuliers, au principe selon lequel un niveau de protection approprié doit être assuré et d'autoriser un transfert donné vers un destinataire n'assurant pas une telle protection. Des telles dérogations ne sont permises que dans des circonstances bien définies : consentement ou intérêt spécifique de la personne concernée et/ou existence d'intérêts légitimes prépondérants et prévus par la loi. Ces intérêts légitimes prépondérants ne sont pas ceux de l'Etat destinataire. Les dérogations doivent respecter le principe de proportionnalité et ne pas être utilisées pour des transferts massifs ou répétitifs. Pour ce type de transferts, les dispositions de l'article 12.3 s'appliquent et des garanties adéquates doivent être mises en place.

110. *Le paragraphe 5* prévoit une garantie complémentaire, à savoir que l'autorité de contrôle compétente reçoit toute information pertinente relative aux transferts de données prévus au paragraphe 3.b, tels que les transferts accompagnés de garanties *ad hoc* ou de garanties standardisées agréées. En particulier, l'autorité sera informée des procédures relatives aux transferts et du contenu des instruments juridiquement contraignants apportant les garanties. Les transferts correspondant aux situations dans lesquelles aucun niveau de protection approprié n'est assuré mais qui sont justifiés par des intérêts spécifiques de la personne concernée (paragraphe 4.b.) ou des intérêts légitimes prépondérants (paragraphe 4.c.) doivent également être soumis au contrôle de l'autorité compétente. L'autorité doit avoir la faculté de demander les informations pertinentes sur les circonstances et la justification de tels transferts.

111. *Aux termes du paragraphe 6,* l'autorité de contrôle doit avoir la faculté d'exiger que l'efficacité des mesures prises ou l'existence d'intérêts légitimes prépondérants soient démontrées et d'interdire, suspendre ou soumettre à des conditions les transferts si cela se révèle nécessaire pour protéger les droits et les libertés fondamentales des personnes concernées.

112. En ce qui concerne les flux transfrontières de données à caractère personnel, des dérogations spécifiques sont permises pour protéger la liberté d'expression, y compris la liberté de la presse. Les Parties peuvent autoriser des exceptions aux dispositions de l'article 12 pour autant qu'elles soient prévues par la loi et nécessaires dans une société démocratique pour protéger la liberté d'expression. Une mesure « nécessaire dans une société démocratique » doit poursuivre un but légitime et donc répondre à un besoin social impérieux qui ne peut être atteint par des moyens moins intrusifs. Une telle mesure doit être proportionnée au but légitime poursuivi et les motifs avancés par les autorités nationales pour la justifier doivent être pertinents et suffisants. Enfin, elle doit être établie par une loi accessible et prévisible, qui doit être suffisamment détaillée.

113. Les flux de données et le nécessaire renforcement de la protection des données à caractère personnel imposent également une coopération internationale accrue entre autorités de contrôle compétentes en vue de l'application des lois.

Chapitre III bis – Autorités de contrôle

Article 12bis – Autorités de contrôle

114. 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 qui disposent de lois de protection des données ont créé des autorités de contrôle pour faire face à la complexité et au caractère évolutif du traitement des données, à la lumière des évolutions organisationnelles, sociales et sociétales. Cela nécessite une entité externe, indépendante et impartiale, dotée d'une grande réactivité et d'une expertise spécialisée, qui peut être un commissaire ou un organe collégial. Les autorités de contrôle dans le domaine de la protection des données fournissent un recours approprié lorsqu'elles sont dotées de pouvoirs et de compétences effectifs et qu'elles jouissent d'une réelle indépendance dans l'exercice de leurs fonctions. Elles forment une composante essentielle du système de contrôle de la protection des données dans une société démocratique.

115. Cet article de la Convention vise à assurer la protection effective de l'individu en demandant aux Parties de créer 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. Le paragraphe 1 précise que plus d'une autorité pourrait être nécessaire pour satisfaire les particularités des différents systèmes juridiques (Etats fédéraux, par exemple). Des autorités de contrôle spécifiques dont l'activité serait limitée à un secteur donné (communications électroniques, santé, secteur public, etc.) pourraient également être mises en place. Ces autorités exerceraient leurs fonctions sans préjudice de la compétence des juridictions ou autres instances chargées de veiller au respect des lois donnant effet aux principes de la Convention. Les autorités de contrôle devraient disposer des infrastructures et ressources financières, techniques et humaines (juristes, spécialistes en technologies de l'information et de la communication) nécessaires pour agir rapidement et efficacement. Il convient de faire régulièrement le point sur ces ressources eu égard à d'éventuels élargissements des pouvoirs et des fonctions.

116. Les Parties disposent d'une certaine marge d'appréciation quant à la façon de mettre en place ces autorités pour qu'elles puissent mener à bien leur mission. Le paragraphe 2 énonce toutefois qu'elles doivent être dotées, au moins, de pouvoirs d'investigation et d'intervention, ainsi que du pouvoir de rendre des décisions et d'infliger des sanctions administratives à des autorités publiques ou à des acteurs du secteur privé. Par ailleurs, elles doivent être consultées dans les processus normatifs législatifs et administratifs concernant la protection des données, être dotées de pouvoirs spécifiques relatifs aux flux de données (notamment l'agrément des garanties standardisées), être habilitées à recevoir les plaintes de particuliers et disposer du pouvoir d'ester en justice ou de porter à la connaissance des autorités judiciaires compétentes toute violation des dispositions applicables. Enfin, elles doivent avoir une mission de sensibilisation à la protection des données.

117. L'autorité doit disposer de pouvoirs d'investigation, tels que la possibilité de demander au responsable du traitement et au sous-traitant des informations concernant le traitement de données à caractère personnel et de les obtenir. En vertu de l'article 8 de la Convention, de telles informations devraient être mises à disposition, en particulier, lorsque l'autorité de contrôle est saisie par une personne entendant exercer les droits énoncés dans cet article.

118. Le pouvoir d'intervention de l'autorité de contrôle, prévu au paragraphe 1, peut prendre diverses formes dans le droit des Parties. Par exemple, l'autorité pourrait avoir la faculté d'obliger le responsable du traitement à rectifier des données inexactes ou collectées de manière illégale, de les effacer ou de les détruire, d'office ou lorsque la personne concernée n'est pas en mesure d'exercer ces droits personnellement. Le pouvoir de demander des ordonnances 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 pourrait également inclure la possibilité de rendre des avis préalables à la mise en œuvre d'opérations de traitement de données (lorsque le traitement présente des risques particuliers pour les droits et les libertés fondamentales, l'autorité de contrôle devrait être consultée par les responsables du traitement dès les premières phases de conception des processus) ou de saisir les parlements nationaux ou d'autres institutions étatiques.

119. Par ailleurs, aux termes du paragraphe 3, toute personne devrait avoir la possibilité de saisir l'autorité de contrôle de toute requête concernant ses droits et libertés à l'égard du traitement de données à caractère personnel. Cela contribue à garantir le droit à un recours approprié, prévu aux articles 8 et 10 de la Convention. Outre ces investigations, en vertu des paragraphes 2(c) et 2(d), les autorités de contrôle peuvent notamment décider d'imposer une sanction administrative ou de porter le dossier devant l'autorité judiciaire compétente en la saisissant ou en engageant des poursuites judiciaires (voir paragraphe suivant). Dans certaines juridictions, les autorités de contrôle n'ont pas qualité pour ester en justice. Le pouvoir d'imposer des sanctions administratives est donc très important pour leurs capacités en matière d'application de la loi. Ces pouvoirs étant conférés aux autorités de contrôle, elles doivent également disposer des ressources nécessaires à leur exercice. En fonction des ressources dont elles disposent, les autorités de contrôle devraient avoir la possibilité de définir des priorités pour le traitement des plaintes et demandes déposées par les personnes concernées.

120. Les Parties devraient donner à l'autorité de contrôle le pouvoir d'ester en justice ou de porter à la connaissance des autorités judiciaires toute violation des règles de protection des données, conformément aux paragraphes 2(c) et 2(d). Ce pouvoir découle du pouvoir d'investigation qui peut conduire l'autorité à constater une violation du droit à la protection garanti à tout individu. L'obligation des Parties d'accorder ce pouvoir à l'autorité de contrôle peut être remplie en l'autorisant à prendre des décisions.

121. Lorsqu'une décision administrative produit des effets juridiques, la personne concernée est en droit de disposer d'un un recours juridictionnel effectif. Néanmoins, le droit interne peut soumettre ce recours à une saisine préalable de l'autorité de contrôle.

122. Le paragraphe 2(e) traite du rôle des autorités de contrôle en matière de sensibilisation Tout en contribuant à la protection des droits de l'individu, l'autorité de contrôle sert de relais entre la personne concernée et le responsable du traitement. Dans ce contexte, il semble particulièrement important que l'autorité de contrôle assure de manière proactive la visibilité de ses activités, fonctions et pouvoirs. Elle devra pour cela informer l'opinion par le biais de rapports périodiques (voir paragraphe 129) ; elle pourra également publier des avis ou utiliser tout autre moyen de communication et formuler publiquement des recommandations au chef de l'Etat, au gouvernement et au Parlement en vue d'améliorer le système de protection des données. Par ailleurs, elle doit fournir des informations aux individus et aux responsables du traitement ainsi qu'aux sous-traitants, sur leurs droits et obligations en matière de protection des données. Dans leur travail de sensibilisation aux questions relatives à la protection des données, les

autorités de contrôle devront veiller à s'adresser spécifiquement aux enfants et aux catégories vulnérables de personnes par des moyens et un langage adaptés.

123. Comme prévu au paragraphe 2bis, les autorités de contrôle doivent pouvoir formuler des avis sur toute mesure législative ou administrative prévoyant le traitement de données à caractère personnel. Seules les mesures générales sont visées par ce pouvoir consultatif, et non les mesures individuelles.

124. L'autorité pourrait également être appelée à donner son avis lorsque d'autres mesures relatives au traitement des données à caractère personnel sont en préparation, par exemple des codes de conduite ou des normes techniques.

125. Les compétences de l'autorité de contrôle ne se limitent pas à celles énoncées à l'article 12bis. Elle peut juger approprié de formuler des recommandations générales sur l'application correcte des règles de protection des données. Elle peut consulter les différentes parties prenantes. Les autorités de contrôle pourraient également tenir un registre des traitements ouvert au public. Enfin, il convient de garder à l'esprit que les Parties ont d'autres moyens de rendre effective la mission de l'autorité de contrôle. Par exemple, l'autorité pourrait être saisie par une association, en particulier lorsque conformément à l'article 9 de la Convention, les droits des personnes représentées par cette dernière font l'objet de restrictions.

126. Le paragraphe 4 précise que les autorités de contrôle ne peuvent protéger efficacement les droits et libertés individuels si elles n'agissent pas en toute indépendance. Plusieurs éléments contribuent à assurer l'indépendance de l'autorité de contrôle dans l'exercice de ses fonctions. Ils devraient inclure : la composition de l'autorité, le mode de désignation de ses membres, la durée d'exercice et les conditions de cessation de leurs fonctions, la possibilité donnée aux 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, l'octroi de ressources suffisantes à l'autorité, la possibilité de recruter ses propres agents conformément à des règles internes ou encore l'adoption de décisions sans injonctions ou ordres extérieurs.

127. L'interdiction de solliciter ou d'accepter des instructions couvre l'accomplissement des fonctions en tant qu'autorité de contrôle. Cela n'empêche pas les autorités de contrôle de demander des avis spécialisés (par exemple auprès de psychologues, de spécialistes des technologies de l'information et de la communication ainsi que d'autres consultants et homologues, etc.) dans les cas où elles l'estiment nécessaire, pour autant qu'elles portent un jugement indépendant.

128. La transparence concernant les travaux et activités des autorités de contrôle est requise, notamment par la publication d'un rapport d'activités annuel comportant entre autres des informations sur les mesures prises pour faire appliquer la loi, conformément au paragraphe 5bis.

129. En contrepartie de cette indépendance, les décisions des autorités de contrôle doivent elles-mêmes pouvoir faire l'objet d'un recours juridictionnel en vertu du principe de la prééminence du droit, comme le prévoit le paragraphe 6.

130. Tout en partant du principe que les autorités de contrôle devraient avoir la capacité juridique d'ester en justice et de demander l'application de la loi, l'intervention (ou l'absence d'intervention) d'une autorité de contrôle ne doit pas faire obstacle à la possibilité pour tout individu concerné d'exercer un recours juridictionnel.

131. Le paragraphe 7 est le premier des trois ensembles de dispositions de la Convention portant sur la coopération entre les Parties par le biais de leurs diverses autorités pour donner effet aux lois de protection des données mises en œuvre en application de la Convention (les autres étant les articles 13-17 sur l'entraide et les articles 18-20 sur le Comité conventionnel). La Convention établit une distinction

entre deux niveaux de coopération : (1) entre les *Parties*, pour le compte desquelles toute autorité désignée peut agir, et (2) entre les *autorités de contrôle*. C'est de cette dernière forme de coopération que traite la présente disposition, tandis que les suivantes portent sur la première.

132. La nécessité d'une coopération entre les Parties, et donc entre diverses juridictions, est principalement imposée par la mondialisation et l'évolution rapide de la technologie, toutes deux à l'origine de transferts simultanés de données à caractère personnel qui augmentent les divers risques pour les personnes et imposent une action coordonnée et rapide. La Convention n'entend pas seulement apporter des réponses *adéquates* à ce besoin, mais également offrir des moyens de coopération qui rendent ces réponses *effectives*. C'est pourquoi elle propose diverses possibilités, contenues dans les trois ensembles de dispositions précités.

133. La notion de coopération n'est pas de nature uniforme et va des formes « strictes » comme l'application des lois en matière de protection des données, où la légalité de l'action de chaque autorité de contrôle est indispensable, à certaines formes plus « souples » comme la sensibilisation, la formation ou l'échange de personnel (cf. « actions conjointes » à l'article 12bis(7)(b)).

134. Les autorités de contrôle ont à la fois le pouvoir et l'obligation d'exercer l'ensemble des fonctions et compétences énoncées à l'article 12bis(2) dès lors qu'un élément extraterritorial entre en jeu, par exemple dans le cas d'une requête individuelle contre un responsable du traitement/sous-traitant qui traite des données à caractère personnel dans plus d'une juridiction.

135. Le catalogue des possibilités de coopération n'est pas exhaustif. En premier lieu, les autorités de contrôle doivent s'accorder mutuellement assistance, notamment par l'échange d'informations pertinentes et utiles, qui peuvent être de deux types : 1) « les informations et documents sur leur droit et sur leur pratique administrative en matière de protection des données », ce qui ne pose habituellement aucune difficulté, ces informations pouvant être échangées librement et être rendues publiques, et (2) les informations confidentielles ou autres informations protégées par le secret - secret d'Etat ou secret professionnel, par exemple - ainsi que les données à caractère personnel.

136. Les données à caractère personnel ne peuvent faire l'objet d'un échange qu'à la condition : (1) qu'elles soient essentielles à la coopération, c'est à dire que la coopération deviendrait inopérante sans ces informations, ou (2) que la personne concernée ait donné son « consentement explicite, spécifique, libre et éclairé pour ce faire ». Dans tous les cas, le transfert de données à caractère personnel doit respecter les dispositions de la Convention, et en particulier son chapitre II (cf. également art. 16(b) concernant les motifs de refus).

137. Les autorités de contrôle peuvent également coopérer en coordonnant leurs investigations ou interventions ou en menant des actions conjointes. Pour les procédures applicables, les autorités de contrôle se réfèreront à la législation de base au niveau national, comme les codes de procédure administrative, civile ou pénale, ou les engagements supranationaux ou internationaux qui lient leurs juridictions, par exemple les traités d'entraide juridique, après examen de leur capacité juridique à prendre part à une telle coopération.

138. Les dispositions sur l'entraide entre autorités de contrôle doivent être lues en parallèle avec les dispositions des articles 13-17, qui s'appliqueraient *mutatis mutandis*.

139. Le paragraphe 8 évoque un réseau d'autorités de contrôle comme moyen de contribuer à la rationalisation du processus de coopération et donc à l'efficacité de la protection des données à caractère personnel. Il est important de noter que la Convention mentionne « un » réseau au singulier. Cette disposition ne semble pas exclure la possibilité, pour les autorités de contrôle des Parties, de s'associer à d'autres réseaux.

140. Afin de protéger l'indépendance des juges dans l'exercice de leurs fonctions juridictionnelles, le paragraphe 9 de l'article 12bis prévoit que les autorités de contrôle ne sont pas compétentes s'agissant des traitements effectués par des organes dans l'exercice de leurs fonctions juridictionnelles. Une telle

dérogation devrait être strictement limitée aux activités judiciaires proprement dites et ne pas s'appliquer aux autres activités que pourraient exercer les juges, conformément au droit interne.

Chapitre IV – Entraide

Article 13 – Coopération entre les Parties

141. Le chapitre IV (articles 13-17) constitue le deuxième ensemble de dispositions sur la coopération entre les Parties par le biais de leurs diverses autorités pour donner effet aux lois de protection des données mises en œuvre en application de la Convention (*cf*. par. **Error! Reference source not found.**). L'entraide est obligatoire. A cette fin, les Parties désignent une ou plusieurs autorités et en communiquent les coordonnées, ainsi que les compétences techniques et territoriales, s'il y a lieu, au Secrétaire Général du Conseil de l'Europe. Les articles suivants établissent un cadre détaillé en matière d'entraide.

142. Bien qu'en principe, la coopération entre les Parties soit assurée de manière générale par les autorités de contrôle établies en vertu de l'article 12bis de la Convention, il ne peut être exclu qu'une Partie désigne une autre autorité pour donner effet aux dispositions de l'article 13.

143. L'article 16(b) permet à une autorité de refuser une demande d'assistance si elle « n'est pas conforme aux dispositions de la présente Convention », les principales dispositions visées ici étant celles du chapitre II.

144. La coopération et l'assistance générale valent pour les contrôles a priori et a posteriori (par exemple pour vérifier les activités d'un responsable du traitement particulier). Les informations échangées pourront être de caractère juridique ou factuel.

Article 14 – Assistance aux personnes concernées

145. Le paragraphe 1 garantit que toute personne concernée, dans une Partie à la Convention ou un pays tiers, peut exercer les droits qui lui sont reconnus à l'article 8 de la Convention indépendamment de son lieu de résidence ou sa nationalité.

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

147. Il va sans dire que les personnes qui résident à l'étranger conservent la possibilité d'exercer leurs droits avec l'aide des agents diplomatiques ou consulaires de leur propre pays.

148. Pour faciliter la procédure, les demandes doivent être aussi précises que possible, conformément au paragraphe 3.

Article 15 – Garanties concernant l'assistance

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

150. Une autorité de contrôle ne peut apporter une assistance au nom d'une personne concernée qu'en réponse à une demande de cette personne. L'autorité doit avoir reçu mandat de la personne concernée et

ne peut agir de sa propre initiative pour le compte de celle-ci. Cette disposition revêt une importance fondamentale pour la confiance réciproque sur laquelle repose l'assistance mutuelle.

Article 16 – Refus des demandes d'assistance

151. Cet article dispose que 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 traités internationaux en matière d'entraide.

152. Le terme « exécution » employé à la lettre c doit s'entendre dans un sens large couvrant non seulement la réponse à la demande, mais également l'activité qui la précède. Ainsi, une autorité saisie d'une demande d'assistance peut refuser d'y donner suite si la transmission de l'information demandée à l'autorité requérante ou plus simplement le fait même de demander l'information risquent de porter préjudice aux droits et libertés fondamentales d'un individu.

Article 17 – Frais et procédures de l'assistance

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

154. La notion d'« experts » au sens du paragraphe 1 englobe les professionnels du traitement des données dont l'intervention est requise pour effectuer des essais de fonctionnement ou vérifier la sécurité des données dans une opération de traitement.

155. Pour ne pas alourdir la Convention par une multitude de détails d'exécution, le paragraphe 3 de cet article prévoit que les formes et procédures ainsi que les langues à utiliser peuvent être convenues entre les Parties concernées. Le libellé de ce paragraphe n'exige pas de procédures formelles mais permet des arrangements administratifs qui peuvent même être limités à des cas spécifiques. Il est souhaitable en outre que les Parties laissent aux autorités désignées le pouvoir de conclure ces arrangements. Les formes de l'assistance pourront également varier d'un cas à l'autre. 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 demandes de routine sur les inscriptions figurant dans un registre de population.

Chapitre V – Comité conventionnel

156. Le but des articles 18, 19 et 20 est de faciliter l'application de la Convention et, le cas échéant, de perfectionner celle-ci. Le Comité conventionnel constitue le troisième moyen de coopération entre les Parties pour donner effet aux lois de protection des données mises en œuvre en application de la Convention (*cf*. par. **Error! Reference source not found.** et 141).

157. Un Comité conventionnel est constitué, composé de représentants de toutes les Parties, issus des autorités de contrôle nationales ou du gouvernement.

158. La nature du Comité conventionnel et ses procédures sont analogues à celles établies aux termes d'autres conventions conclues dans le cadre du Conseil de l'Europe.

159. La Convention portant sur un thème en constante évolution, on peut s'attendre à ce que des questions se posent tant en ce qui concerne son application pratique (article 19, lettre a) que son interprétation (même article, lettre d).

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

161. Le Comité conventionnel jouera un rôle clé dans l'évaluation du respect de la Convention, soit par la préparation d'une évaluation du niveau de protection des données offert par un candidat à l'adhésion (article 19, lettre e) soit par l'examen périodique de l'application de la Convention par les Parties (article 19, lettre h), le but visé étant de garantir la mise en œuvre des principes de protection des données consacrés par la Convention et de parvenir à une harmonisation du niveau élevé de protection dans les Parties à la Convention. Le Comité conventionnel aura également la faculté d'évaluer la conformité avec la Convention du régime de protection des données d'un Etat ou d'une organisation internationale (article 19, lettre f).

162. Lorsqu'il fournira de tels avis sur le degré conformité avec la Convention, le Comité conventionnel conduira ses travaux sur la base d'une procédure équitable, transparente et publique décrite de façon détaillée dans son règlement.

163. Il aura également la faculté d'approuver des modèles de garanties standardisées pour les transferts de données (article 19, lettre g).

164. Enfin, il pourra contribuer au règlement de toute difficulté surgissant entre les Parties (article 19 lettre i). En cas de différends, le Comité conventionnel s'efforcera de parvenir à un règlement par la négociation ou tout autre moyen amiable.

Chapitre VI – Amendements

Article 21 – Amendements

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

166. 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).

167. 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

168. Un large champ d'application géographique étant 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 ou d'organisations internationales

169. La Convention, qui a été élaborée à l'origine en étroite collaboration 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 d'évaluer la conformité et de préparer un avis pour le Comité des Ministres concernant le degré de protection des données du candidat à l'adhésion.

170. Les flux de données ne connaissant pas de frontières, l'adhésion de pays et d'organisations internationales du monde entier est recherchée. Sont seules susceptibles d'adhérer à la Convention les organisations internationales définies comme organisations intergouvernementales (Convention de Vienne de 1986 sur le droit des traités entre Etats et organisations internationales ou entre organisations internationales).

Article 24 – Clause territoriale

171. 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, que ce soit pour des raisons de coût et de main-d'œuvre ou pour la capacité de traitement en alternance jour/nuit.

Article 25 – Réserves

172. 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 à ses dispositions, qui offrent toutefois une souplesse raisonnable compte tenu des dérogations admises par certains articles.

Article 26 – Dénonciation

173. Conformément à l'article 80 de la Convention des Nations Unies de Vienne sur le droit des traités, toute partie peut dénoncer la Convention.

Article 27 – Notification

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