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

## PROJET DE RAPPORT EXPLICATIF[1]

Le présent document a été préparé sur la base du texte consolidé des propositions de modernisation de la Convention 108 (voir document GR-J(2016)14) : la numérotation des articles ne correspond pas au projet de protocole d'amendement de la Convention.

## I. INTRODUCTION

1. Depuis son ouverture à la signature il y a plus de trente-cinq ans, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dénommée Convention 108 (ci-après « la Convention » également) a servi de fondation au cadre juridique international en matière de protection des données dans plus de 40 pays européens. Elle a influencé également les politiques et les législations bien au-delà des frontières de l'Europe. Avec de nouveaux défis voyant le jour quotidiennement 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.

2. Un large consensus sur les aspects suivants de la modernisation de la Convention a vu le jour : 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.

3. 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 (révisées en 2013) 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

[1] La présente version du projet a été préparée sur la base de consultations écrites ainsi que de la réunion informelle qui s'est tenue le 24 août 2016.

Pendant cette réunion informelle, la Délégation de la Fédération de Russie a fait la déclaration suivante:

**"**Au vu du fait que plusieurs questions relatives aux Articles 9, 12 et 20 du projet de modernisation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) n'ont pas été résolues lors de la 4ème réunion du Comité ad hoc sur la protection des données (CAHDATA) et demeurent non résolues à ce jour, la Fédération de Russie considère qu'il est prématuré de traiter des dispositions du projet de rapport explicatif à la Convention qui correspondent à ces articles. A cet égard, la Fédération de Russie met en attente ses commentaires sur ces dispositions du projet de rapport explicatif jusqu'à ce qu'un accord sur ces articles soit trouvé et le texte finalisé.
Par ailleurs, la Fédération de Russie souhaite souligner que la version du projet de rapport explicatif approuvée par le Groupe n'exclut pas la possibilité d'amender les dispositions du rapport relatives aux Articles susmentionnés, ni ne prédétermine en aucune façon la substance de ces Articles.
La Fédération de Russie se réserve la possibilité de formuler des commentaires et propositions sur le rapport le moment venu sous réserve de la réalisation des conditions susmentionnées."

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 (UE) (à partir de 1995[2]), 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[3]. S'agissant de la réforme du cadre législatif en matière de protection des données de l'UE en particulier, les travaux ont été menés en parallèle et la plus grande attention a été portée au maintien de la cohérence entre les deux cadres législatifs. Le cadre de l'UE en matière de protection des données précise et amplifie les principes de la Convention 108 et prend en considération l'adhésion à la Convention, notamment au regard des transferts internationaux[4].

4. Le comité consultatif constitué en application de l'article 18 de la Convention a préparé le projet de propositions de modernisation qui a été adoptés à sa 29e réunion plénière (27-30 novembre 2012) et soumis au Comité des Ministres qui a ensuite chargé le Comité *ad hoc* sur la protection des données (CAHDATA) de les finaliser. Ce travail a été terminé à l'occasion de la 3e 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. La dernière réunion du CAHDATA (15-16 juin 2016) a finalisé les propositions et les a transmises au Comité des Ministres pour examen et adoption.

5. 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. Les obligations légales des Parties découlent du texte de la Convention et aucune disposition du présent rapport ne peut être entendue comme restreignant, limitant ou étendant les droits et obligations prévus par la Convention.

Le présent Protocole a été ouvert à la signature à ..., le ... .

## II. COMMENTAIRES

6. Le but du présent Protocole est de moderniser 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.

7. Les rapports explicatifs de la Convention 108 et de son protocole additionnel conservent toute leur pertinence dans la mesure où ils exposent le contexte historique et décrivent l'évolution qui a conduit à l'adoption de ces deux instruments. Ils peuvent à ce titre être lus conjointement avec le présent document.

### Préambule

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

9. 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 qu'opèrent 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

[2] Règlement général sur la protection des données (UE) 2016/679 (« RGPD ») et Directive relative à la protection des données à caractère personnel dans le secteur de la police et de la justice pénale (UE) 2016/680 (« Directive Police »).
[3] 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.
[4] Voir en particulier le considérant 105 du RGPD.

privée, ainsi que la dignité de la personne. La dignité humaine requiert 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.

10. 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, le cas échéant, de concilier les intérêts, droits et libertés fondamentales des individus. C'est afin de maintenir un juste équilibre entre les intérêts, droits et libertés fondamentales que la Convention prévoit des mesures et restrictions à l'égard du traitement d'informations et la protection des données à caractère personnel. Le droit à la protection des données doit notamment être considéré aux côtés du droit à la liberté d'expression consacré par l'article 10 de la Convention européenne des droits de l'homme, qui 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[5].

11. La Convention 108, à travers les principes qu'elle énonce et les valeurs qu'elle contient, protège l'individu tout en définissant un cadre pour les flux internationaux de données. Ce point est important car les flux internationaux d'informations jouent un rôle de plus en plus significatif pour la société moderne, permettant l'exercice des droits et libertés fondamentales tout en suscitant l'innovation et en encourageant le progrès social et économique, tout en jouant également un rôle vital pour la sécurité publique. La circulation des données à caractère personnel dans une société de l'information et de la communication doit respecter les droits et libertés fondamentales des individus. Ces droits doivent également être respectés lors du développement et 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.

12. 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 exigeant des Parties qu'elles se prêtent 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

13. 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.[6] La protection des données à caractère personnel a plus récemment été introduite comme un droit fondamental à l'article 8 de la Charte des droits fondamentaux de l'UE ainsi que dans les constitutions de plusieurs Parties à la Convention.

14. 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[7]. 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.

[5] Voir Convention du Conseil de l'Europe sur l'accès aux documents publics (STCE n° 205).

[6] « 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 », Cour européenne des droits de l'homme, *MS c. Suède* 1997 par. 41.

[7] 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.

## Article 2 – Définitions

15. 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 »*

16. 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 efforts ou des ressources déraisonnables. Tel est le cas lorsque l'identification de la personne concernée exige des opérations excessivement complexes, longues et coûteuses. Estimer ce qui constitue des « délais, des efforts ou des ressources déraisonnables » doit être considéré au cas par cas. Par exemple en tenant notamment compte 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. Par ailleurs, les avancées technologiques et autres développements peuvent influer sur ce que revêt la notion de « délais, efforts ou ressources déraisonnables ».

17. 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. La qualité des techniques de pseudonymisation appliquées lors du traitement des données devrait être dûment prise en compte lors de l'évaluation de la pertinence des garanties mises en place afin de réduire les risques pour les personnes concernées.

18. Les données ne peuvent être considérées comme anonymes que lorsque la ré-identification de la personne concernée est impossible ou nécessiterait des délais, efforts ou ressources déraisonnables, au vu des technologies disponibles au moment du traitement et de l'évolution de celles-ci. 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 ressources déraisonnables) permettre l'identification d'une personne. C'est notamment le cas lorsque la combinaison de différents types de données, telles que des données physiques, physiologiques, génétiques, économiques ou sociales (combinaison de données relatives à 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.

19. Lorsque des données sont rendues anonymes, des moyens appropriés 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, ces moyens techniques devraient être réévalués régulièrement.

*Lettres b et c – « traitement de données »*

20. Le « traitement de données » commence par la collecte de données à caractère personnel et englobe toutes les opérations effectuées sur les données, qu'elles le soient de façon totalement automatisée ou en

partie seulement. Lorsque aucun procédé automatisé n'est utilisé, le traitement de données désigne une opération ou des opérations effectuée(s) sur des données à caractère personnel au sein d'un ensemble structuré de données qui sont accessibles ou peuvent être retrouvées selon des critères spécifiques ou qui permettent au responsable du traitement ou à toute autre personne de rechercher, combiner ou mettre en corrélation des données relatives à une personne.

*Lettre d – « responsable du traitement »*

21. « Responsable du traitement » désigne la personne ou l'organe qui dispose du pouvoir de décision à l'égard des finalités et moyens 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). Afin de déterminer si un organe ou une personne peuvent être qualifiés de responsable du traitement, une attention particulière doit être portée au fait de savoir si il ou elle détermine les motifs justifiant le traitement, à savoir ses finalités, ainsi que les moyens utilisés. D'autres facteurs pertinents dans cet exercice de qualification comprennent le fait de contrôler ou non les méthodes du traitement, le choix des données à traiter et les personnes autorisées à y accéder. Les personnes qui ne sont pas directement subordonnées au responsable du traitement et qui effectuent le traitement pour son compte, conformément à ses instructions, sont des sous-traitants. Le responsable du traitement conserve la responsabilité du traitement lorsque ce dernier est effectué pour son compte par un sous-traitant.

*Lettre e – « destinataire »*

22. « Destinataire » désigne la personne ou l'entité qui reçoit des données à caractère personnel ou à qui ces données sont rendues accessibles. Selon le cas, le destinataire peut être un responsable du traitement ou un sous-traitant. Par exemple, une entreprise peut envoyer certaines 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. Le destinataire peut être un organisme public ou une entité qui s'est vue reconnaître le droit d'exercer une fonction publique mais lorsque les données reçues par cet organisme ou entité sont traitées dans le cadre d'une demande particulière conformément au droit applicable, cet organisme ou entité ne sera pas considéré comme un destinataire. Les demandes de communication faites par les autorités publiques devraient toujours être présentées par écrit, être motivées et revêtir un caractère occasionnel, et elles ne devraient pas porter sur l'intégralité d'un fichier ni conduire à l'interconnexion de fichiers. Le traitement des données à caractère personnel par les autorités publiques en question devrait être effectué dans le respect des règles applicables en matière de protection des données en fonction des finalités du traitement.

*Lettre f – « sous-traitant »*

23. Le « sous-traitant » est toute personne physique ou morale (autre que les employés du responsable du traitement) qui accomplit les opérations de traitement pour le compte 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.

**Article 3 – Champ d'application**

24. Conformément au paragraphe 1, chaque Partie s'engage à appliquer la Convention à tout traitement de données relevant de sa juridiction[8], dans le secteur public comme dans le secteur privé. Tout traitement de données effectué par un établissement public relève directement de la juridiction de la

[8] 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.

Partie concernée, étant le produit de l'exercice de ses compétences. Les traitements de données effectuées par des responsables du 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.

25. 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 de permettre de s'adapter aux progrès technologiques constants[9].

26. *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 sont exclusivement liées 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. Le partage de données au sein de la « sphère privée » comprend notamment le partage fait au sein de la famille, d'un cercle restreint d'amis ou d'un cercle limité en taille, basé sur une relation personnelle ou une relation de confiance particulière.

27. 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 »[10].

28. 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.

29. 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.

---

[9] 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. ».
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.

[10] Voir Cour de Justice de l'UE, 11 décembre 2014, (František Ryneš contre Úřad) C-212/13.

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

### Article 4 – Engagements des Parties

30. Comme l'indique cet article, la Convention oblige les Parties à intégrer dans leur « loi » les dispositions de la Convention et de veiller à leur application effective en pratique. La façon dont cette intégration est effectuée dépend du système juridique applicable et de l'effet qu'il reconnaît aux traités internationaux en droit interne.

31. 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 répondre 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 toute personne susceptible d'être concernée par cette loi doit y avoir accès. L'expression 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'UE. 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.

32. La « loi des Parties » peut être complétée 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.

33. S'agissant des organisations internationales[11], le droit interne de ces organisations peut dans certaines situations être appliqué directement au niveau national dans chacun des Etats membres, en fonction des systèmes juridiques nationaux.

34. L'efficacité de l'application des mesures prises pour donner effet aux dispositions de la Convention revêt une importance fondamentale. 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.

35. Il est en outre énoncé au paragraphe 2 que les mesures donnant effet à la Convention 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 et de 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.

[11] Les organisations internationales sont définies comme des organisations soumises au droit public international.

36. Les Parties s'engagent, au paragraphe 3, 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 de rapports sur l'application de la législation en matière de protection des données pourrait être un élément de cette contribution active des Parties.

37. 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**

38. Le paragraphe 1 dispose que le traitement des données doit être proportionné, c'est-à-dire pertinent au regard de la finalité légitime poursuivie, et limité à ce qui est nécessaire au regard des intérêts, droits et libertés des personnes concernées ou de l'intérêt public. Il ne doit pas induire une ingérence disproportionnée dans ces intérêts, droits et libertés. 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.

39. Le paragraphe 2 prévoit que la licéité 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, 3 et 4 de l'article 5 sont cumulatifs et doivent être respectés pour garantir la légitimité du traitement des données.

40. Le consentement de la personne concernée doit être libre, spécifique, éclairé et non équivoque. Un tel consentement doit représenter 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 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 pré-validés 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 informée des implications de sa décision (ce que signifie le fait de donner son consentement et l'étendue de ce dernier). Aucune influence ou pression indues (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 subir de préjudice.

41. En matière de recherche scientifique, il arrive fréquemment qu'il ne soit pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Par conséquent, les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet.

42. 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 considérée.

43. 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 que le responsable du traitement ait été informé du retrait du consentement mais n'autorise plus la continuation du traitement des données, à moins que cela ne soit justifié par un autre fondement légitime prévu par la loi.

44. 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.

45. 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 défense, 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[12]. Le traitement de données à caractère personnel par des autorités publiques aux fins de réaliser les objectifs, prévus par le droit constitutionnel ou le droit international public, d'associations à caractère religieux officiellement reconnues peut également être considéré comme étant effectué pour des motifs d'intérêt public.

46. Les conditions d'un traitement légitime sont énoncées aux paragraphes 3 et 4. Les données doivent être traitées licitement, loyalement et de manière transparente. 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.

47. La notion d'utilisation « compatible » ne doit pas nuire à la transparence, à la sécurité juridique, à la prédictibilité ou à la loyauté 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. Afin d'établir si les finalités d'un traitement ultérieur sont compatibles avec celles pour lesquelles les données à caractère personnel ont été collectées initialement, le responsable du traitement, après avoir respecté toutes les exigences liées à la licéité du traitement initial, devrait tenir compte, entre autres : de tout lien entre ces finalités et les finalités du traitement ultérieur prévu; du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le

[12] 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.

responsable du traitement, quant à l'utilisation ultérieure desdites données; la nature des données à caractère personnel; les conséquences pour les personnes concernées du traitement ultérieur prévu; et l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu.

48. Le traitement ultérieur des données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, 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 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 excluent, en principe, 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 agrégés. Les statistiques visent à analyser et à caractériser des phénomènes collectifs ou de masse dans une population donnée[13]. Le traitement de données à des fins statistiques peut aussi bien être effectué par le secteur public que le secteur privé. Le traitement de données *« à des fins de recherche scientifique »* 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[14]. Les fins « *de recherche historique* » incluent la recherche généalogique. Les fins « *archivistiques dans l'intérêt public* » peuvent également concerner les archives provenant d'entités privées qui revêtent un caractère d'intérêt public.

49. 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.

50. 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 à ce qui est nécessaire par rapport aux finalités pour lesquelles elles sont traitées. Elles ne devraient être traitées que dans la mesure où ces finalités ne peuvent être raisonnablement 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.

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

52. Des exceptions à l'article 5 paragraphe 4 sont permises de façon limitée et sous réserve des conditions prévues à l'article 9 paragraphe 1.

[13] Recommandation (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.

[14] Exposé des motifs de la Recommandation (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.

**Article 6 – Catégories particulières de données**

53. Le traitement de certaines catégories de données ou le traitement de certaines 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 ne devrait être autorisé que si la loi prévoit des garanties appropriées qui complètent les autres dispositions protectrices de la Convention. L'exigence de garanties appropriées, venant compléter celles de la Convention, n'exclut pas la possibilité, prévue par l'article 9, d'apporter des exceptions ou restrictions aux droits des personnes concernées, énumérés à l'article 8.

54. 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 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).

55. 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.

56. 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.

57. Le contexte du traitement d'images est déterminant dans la qualification de la nature sensible du traitement. Le traitement d'images n'emporte pas, en général, un traitement de données sensibles, les images 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 ethnique, ou sur 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 aux seules fins de sécurité dans une zone commerciale ne sera généralement pas considéré comme tel.

58. 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. Les informations sur la santé englobent 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 d'images de personnes qui portent des lunettes, ont une jambe cassée ou

présentent des brûlures ou toute autre caractéristique visible liée à la santé ne pourra être considéré comme un traitement de données sensibles que si le traitement repose sur des données de santé pouvant être extraites des images.

59. Lorsque des données sensibles doivent être traitées à des fins statistiques, 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. 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 ou longitudinales, par exemple), des garanties appropriées doivent être mises en place[15].

**Article 7 – Sécurité des données**

60. 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.

61. Les mesures de sécurité devraient prendre en considération 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 devraient être revues et actualisées lorsque cela s'avère nécessaire.

62. Les mesures de sécurité visent à prévenir de nombreux risques. Cela dit, le paragraphe 2 contient une obligation spécifique 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, ou susceptible d'entraîner un préjudice financier, une atteinte à la réputation ou des dommages corporels ou une humiliation, pourrait être jugée constitutive d'une atteinte « grave ».

63. En cas de violation de données à caractère personnel, le responsable du traitement est tenu de notifier l'incident aux autorités de contrôle compétentes, sous réserve de l'exception prévue à l'article 9 paragraphe 1. C'est l'exigence minimale. Le responsable du traitement devrait également informer l'autorité de contrôle de toute mesure prise ou proposée pour remédier à la violation et pallier les conséquences potentielles.

64. 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 prendre en considération le besoin d'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. Lorsque 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 souhaitable.

[15] Voir la Recommandation (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.

### Article 7bis – Transparence du traitement

65. Le responsable du traitement est tenu de 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.

66. Le responsable du traitement doit fournir de façon proactive certaines informations essentielles aux personnes concernées lorsqu'il collecte leurs données, directement ou indirectement (c'est-à-dire pas directement auprès des personnes concernées mais auprès d'un tiers). Les informations sur le nom et l'adresse du responsable du traitement (ou co-responsables), la base légale et les finalités du traitement effectué, les catégories de données traitées et leurs destinataires 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.) dès lors qu'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 ou qui serait utile en ce sens, comme la durée de conservation des données, connaître le raisonnement qui sous-tend le traitement des données ou des informations sur les transferts de données vers une Partie à la Convention ou non-Partie (notamment sur la question de savoir si cette non-Partie offre ou non un niveau de protection approprié ou sur les mesures prises par le responsable du traitement pour garantir un tel niveau de protection) devra également être fourni.

67. Le responsable du traitement n'est pas tenu de fournir ces informations lorsque la personne concernée les a déjà reçues, ou dans le cas d'une collecte indirecte de données par le biais de tiers lorsque le traitement est expressément prévu par la loi, 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 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).

68. Le responsable du traitement peut utiliser tous les moyens disponibles, raisonnables et économiquement abordables pour informer les personnes concernées, de façon collective (par un site web ou une campagne de publicité) ou individuellement. Lorsque cela s'avère impossible au début du traitement des données, 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

69. Cet article établit la liste des droits que chaque personne doit être en mesure d'exercer relativement au traitement de données à caractère personnel la concernant. Chaque Partie doit s'assurer, au moyen de son droit interne, que toute personne concernée puisse bénéficier de chacun de ces droits, et qu'elle dispose des moyens nécessaires, adéquats, légaux effectifs et pratiques de les exercer.

70. Ces droits comprennent pour toute personne concernée :

– le droit de ne pas être soumise à une décision l'affectant de manière significative, qui serait prise uniquement sur le fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte (lettre a) ;
– le droit d'obtenir à sa demande, à intervalle raisonnable et sans délai ou frais excessifs, la confirmation de l'existence d'un traitement la concernant et d'accéder aux données traitées (lettre b) ;
– le droit d'obtenir, à sa demande, connaissance du raisonnement qui sous-tend le traitement de données lorsque les résultats de ce traitement lui sont appliqués (lettre c) ;
– le droit de s'opposer, pour des raisons tenant à sa situation, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement à moins que le responsable du traitement ne

démontre des motifs légitimes justifiant le traitement qui prévalent sur ses intérêts, ou ses droits et libertés fondamentales (lettre d) ;
– le droit de rectification ou d'effacement de données inexactes, erronées, ou 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).

71. 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, prévues par une loi, que celles qui constituent des mesures nécessaires et proportionnées dans une société démocratique. Ainsi, le droit d'effacement des données personnelles peut avoir à être limité lorsque le traitement est nécessaire au respect d'une obligation légale à laquelle est soumis le responsable du traitement, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement,

72. Bien que 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, il s'agira, dans la plupart des cas, du responsable du traitement des données ou du sous-traitant qui l'exécute pour son compte. Dans des circonstances exceptionnelles, les moyens d'exercer les droits d'accès, de rectification et d'effacement peuvent impliquer 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.

73. *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, en conduisant à la limitation d'un droit, au refus d'un avantage social ou à l'évaluation de leur capacité d'emprunt sur le seul fondement du logiciel, a pour effet de stigmatiser des individus. La personne concernée ne pourra néanmoins pas exercer ce droit si la décision automatisée est prévue par la loi à laquelle le responsable du traitement est soumis, qui prévoit des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée.

74. *Lettre b.* Les personnes concernées doivent avoir connaissance du traitement de leurs données à caractère personnel. Le droit d'accès devrait en principe être gratuit. La lettre b est toutefois rédigée de manière à permettre au responsable du traitement, dans certaines conditions spécifiques, de demander des frais raisonnables lorsque les demandes sont excessives et vise à couvrir les différentes formules pouvant être adoptées par les Parties selon les cas. 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, ou le sous-traitant, peut également refuser de répondre à des demandes manifestement infondées ou excessives, en raison notamment de leur caractère répétitif. Il incombe alors au responsable du traitement de motiver un tel refus. 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.

75. *Lettre c.* Les personnes concernées ont le droit d'obtenir connaissance du raisonnement qui sous-tend le traitement de données, y compris les conséquences de ce raisonnement et les conclusions qui peuvent en avoir été tirées, en particulier lors de l'utilisation d'algorithmes pour une prise de décision automatisée, notamment dans le cadre du profilage. 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. La compréhension de ces éléments contribue à l'exercice effectif d'autres garanties essentielles comme le droit d'opposition et le droit de recours auprès de l'autorité compétente.

76. *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. Ainsi, la constatation, l'exercice ou la défense d'un droit en justice ou des motifs de sécurité publique 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. Le droit d'opposition opère d'une manière distincte et indépendante des droits de rectification ou d'effacement (Lettre e).

77. 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.

78. Le droit d'opposition peut être limité par la loi, par exemple aux fins de l'investigation ou de la répression d'infractions pénales. La personne concernée peut dans ce cas décider de contester la licéité du traitement. Lorsque le traitement des données repose sur un consentement valablement donné par la personne concernée, le droit de retirer son consentement peut être exercé plutôt que le droit d'opposition. Une personne concernée qui retire son consentement doit alors assumer les conséquences pouvant découler d'autres textes juridiques, comme l'obligation de dédommager le responsable du traitement. De la même façon, lorsque le traitement est fondé sur un contrat, la personne concernée peut prendre les mesures nécessaires à la rupture de ce contrat.

79. *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.

80. *La lettre g* vise à assurer une protection effective des personnes concernées en leur donnant droit à l'assistance d'une autorité de contrôle dans l'exercice des droits prévus par la Convention. Lorsque la personne concernée réside sur le territoire d'une autre Partie, elle peut présenter sa demande par l'intermédiaire de l'autorité désignée par cette Partie. La demande d'assistance doit contenir les informations nécessaires à l'identification du traitement concerné. Ce droit peut être limité en application de l'article 9 ou aménagé pour préserver les intérêts d'une procédure judiciaire en cours.

81. Des exceptions à l'article 8 sont permises de façon limitée et sous réserve des conditions prévues à l'article 9 paragraphe 1.

**Article 8bis - Obligations complémentaires**

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

83. 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 d'être en mesure 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, visent à protéger les personnes concernées et sont également un moyen de renforcer leur confiance. Parmi les mesures appropriées que le responsable du traitement et le sous-traitant peuvent avoir à prendre afin d'être en conformité figure : 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 visant à donner effet à la Convention, ainsi que la mise en place de procédures internes permettant la vérification et la démonstration de la conformité.

84. 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 « délégué à la protection des données » disposant des moyens nécessaires à l'accomplissement de son mandat. 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.

85. *Le paragraphe 2* précise qu'avant d'effectuer une activité de traitement, le responsable du traitement doit examiner son impact potentiel sur les droits et libertés fondamentales des personnes concernées. Cet examen peut être fait sans formalités excessives. Il évaluera également le respect du principe de proportionnalité, en s'appuyant sur une présentation détaillée du traitement envisagé. Dans certains cas, lorsqu'un sous-traitant intervient en plus du responsable du traitement, ce sous-traitant peut également avoir à procéder à un examen des risques. Des développeurs de systèmes d'information, et notamment des spécialistes de la sécurité ou des concepteurs ainsi que des usagers et des juristes peuvent prêter assistance dans l'examen des risques.

86. 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 idéalement 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 aux droits des personnes concernées (protection des données par défaut), notamment afin d'éviter de traiter plus de données qu'il n'est nécessaire pour atteindre la finalité légitime. 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.

87. *Le paragraphe 4* autorise les Parties à 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 adaptées, 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 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 concernées.

### Article 9 – Exceptions et restrictions

88. Aucune exception aux dispositions du chapitre II n'est admise, sauf pour un nombre limité d'entre elles (articles 5.4, 7.2, 7bis paragraphe 1 et article 8), à condition qu'elles soient prévues par la loi, qu'elles respectent l'essence des droits et libertés fondamentales et soient nécessaires, dans une société

démocratique, aux motifs dont la liste 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 adéquats. Enfin, elle doit être établie par une loi accessible et prévisible, qui doit être suffisamment détaillée.

89. Tout traitement de données à caractère personnel doit être licite, loyal et transparent à l'égard des personnes concernées et n'être effectué qu'aux fins spécifiques fixées par la loi. Cela n'interdit pas en soi aux autorités répressives de mener des activités telles que des enquêtes discrètes ou de la vidéosurveillance. Ces activités peuvent être menées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, pour autant qu'elles soient déterminées par la loi et qu'elles constituent une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des intérêts légitimes de la personne concernée.

90. La nécessité de telles exceptions doit être examinée au cas par cas et au regard des objectifs essentiels d'intérêt public général, comme indiqué aux lettres a et b du premier paragraphe. La lettre *a* énumère des objectifs d'intérêt public général de l'Etat ou de l'organisation internationale qui peuvent exiger des exceptions.

91. La notion de « sécurité nationale » s'entend au sens de la protection de la souveraineté nationale de la Partie concernée, à la lumière de la jurisprudence pertinente de la Cour européenne des droits de l'homme[16].

92. L'expression « intérêts économiques et financiers importants » 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 et exécution des sanctions pénales» contenue dans cette lettre inclut les poursuites pénales et l'application des sanctions correspondantes. L'expression « autres objectifs essentiels d'intérêt public général » couvre notamment la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière et l'exécution des demandes de droit civil.

93. *La lettre b* concerne les droits et libertés fondamentales 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 journalistique,

[16] La jurisprudence pertinente comprend en particulier la protection de la sûreté de l'Etat et de la démocratie constitutionnelle contre notamment 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. (Voir Division de recherche de la Cour européenne des droits de l'homme, « Sécurité nationale et jurisprudence européenne », novembre 2013). 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 (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). L'individu doit pouvoir contester l'affirmation de l'exécutif selon laquelle la sécurité nationale se trouve menacée (Cour européenne des droits de l'homme, *Al-Nashif c. Bulgarie*, n° 50963/99, 20 juin 2002). Toute personne qui fait l'objet d'une mesure basée sur des motifs de sécurité nationale doit bénéficier de garanties contre l'arbitraire (Cour européenne des droits de l'homme, *Dalea c. France* (déc.), 964/07, 2 février 2010). 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 (Cour européenne des droits de l'homme, *Segerstedt-Wiberg et autres c. Suède*, n° 62332/00, CEDH 2006-VII).

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. Ceci devrait s'appliquer notamment aux traitements de données à caractère personnel dans le domaine de l'audiovisuel et dans les documents d'archives d'actualités et bibliothèques de la presse. Pour tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique, il y a lieu de retenir une interprétation large des notions liées à cette liberté, telles que le journalisme.

94. Le deuxième paragraphe donne la possibilité de restreindre les dispositions des articles 7bis et 8 pour certains traitements de données effectués à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques qui ne posent aucun risque reconnaissable pour les droits et libertés fondamentales des personnes concernées. Par exemple, cela peut être le cas avec l'utilisation de données pour des travaux statistiques, dans le domaine public comme dans le domaine privé, dans la mesure où ces données sont publiées sous une forme agrégée et à condition que des garanties appropriées en matière de protection des données soient en place (voir paragraphe 48).

95. Les exceptions additionnelles prévues aux articles 12 et 12 bis relatives aux activités de traitement à des fins de sécurité nationale et de défense sont sans préjudice des exigences applicables en matière d'indépendance et d'effectivité des mécanismes de contrôle et de supervision.[17]

**Article 10 – Sanctions et recours**

96. 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.

97. 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 par voie juridictionnelle 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 matériels et le cas échéant d'ordre moral provoqués par le traitement des données, ainsi que des recours collectifs, peuvent également être envisagés.

**Article 11 – Protection plus étendue**

98. 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. L'expression « protection plus étendue » se réfère donc à un niveau de protection qui est supérieur, et non inférieur à celui prévu par la Convention.

[17] Pour les Parties qui sont membres du Conseil de l'Europe, ces exigences découlent de la jurisprudence de la Cour européenne des droits de l'homme, relative à l'article 8 de la Convention européenne des droits de l'homme (voir en particulier les arrêts Roman Zakharov c. Russie, 4 décembre 2015, paragraphe 233 et Szabó et Vissy c. Hongrie, 12 janvier 2016, paragraphes 75 et suivants).

## Chapitre III – Flux transfrontières de données à caractère personnel

### Article 12 – Flux transfrontières de données à caractère personnel

99. 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. Un transfert transfrontière de données intervient lorsque des données à caractère personnel sont communiquées ou mises à disposition d'un destinataire relevant de la juridiction d'un autre Etat ou d'une autre organisation internationale.

100. 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), qui relèvent ensuite de la juridiction d'un Etat non partie à la Convention continuent d'être traitées avec des garanties appropriées. L'important est que les données traitées dans la juridiction d'une Partie soient toujours protégées par les principes pertinents de la Convention. 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.

101. L'article 12 s'applique à l'exportation de données et non pas à leur importation, dans la mesure où dans ce dernier cas, les données relèvent 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, aux seules fins de la protection des données à caractère personnel, 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 notamment le cas des Etats membres de l'UE. Ils sont liés par les règles adoptées au niveau de l'UE qui s'appliquent aux flux transfrontières de données. Cette disposition vise à faire en sorte que toutes les Parties, 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. *Le paragraphe 2* traite des 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 doit être assuré. Dans le cas de destinataires n'est pas Partie à la Convention, la Convention établit deux mécanismes visant à 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.

104. 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 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.

105. 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.

106. 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.

107. *Le paragraphe 4* permet aux Parties de déroger au principe selon lequel un niveau de protection approprié doit être assuré et d'autoriser un transfert 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 et/ou le transfert constitue une mesure nécessaire et proportionnée dans une société démocratique pour la liberté d'expression. Ces dérogations doivent respecter les principes de nécessité et de proportionnalité.

108. *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, et sur demande 4.b et 4.c. L'autorité doit avoir la faculté de demander les informations pertinentes sur les circonstances et la justification de tels transferts. Des exceptions à l'article 12 paragraphe 5 sont permises dans le respect des conditions prévues à l'Article 9 paragraphe 3.

109. *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. Conformément aux conditions prévues à l'article 9 paragraphe 3, des exceptions à l'article 12 sont autorisées.

110. L'augmentation constante des 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

111. Cet article vise à assurer la protection effective des individus en demandant aux Parties de créer une ou plusieurs autorités de contrôle, indépendantes, impartiales et publiques, qui contribuent à la protection des droits et libertés des individus à l'égard du traitement des données à caractère personnel. Il peut s'agir d'un commissaire ou d'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. D'autres mécanismes indépendants et effectifs de contrôle et de supervision des activités de traitement peuvent être prévus par les Parties dans la mesure où l'article 9 paragraphe 3 est appliqué.

112. 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. 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. Le caractère adéquat de leurs ressources doit être gardé sous examen. L'article 9 paragraphe 3 autorise les exceptions aux pouvoirs des autorités de contrôle en matière d'activités de traitement à des fins de sécurité nationale et de défense (dans la mesure ou une telle exception est appliquée d'autres paragraphes du présent article peuvent, par voie de conséquence, devenir non-applicables ou non pertinents). Ceci est néanmoins sans préjudice des exigences applicables en matière d'indépendance et d'effectivité des mécanismes de contrôle et de supervision.[18]

113. 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, sous réserve de la possibilité de prévoir des exceptions conformément à l'article 9 paragraphe 3, être dotées, au moins, de pouvoirs d'investigation et d'intervention, ainsi que du pouvoir de rendre des décisions au regard des violations des dispositions de la Convention. Ceci peut comprendre l'imposition de sanctions administratives, notamment d'amendes. Lorsque le système juridique de la Partie ne prévoit pas l'imposition de sanctions administratives, le paragraphe 2 peut être appliqué de sorte à ce que la sanction soit proposée par l'autorité de contrôle compétente et prononcée par l'autorité judiciaire compétente. Toute sanction imposée doit en tout état de cause être effective, proportionnée et dissuasive.

114. L'autorité doit disposer de pouvoirs d'investigation, sous réserve de la possibilité de prévoir des exceptions conformément à l'article 9 paragraphe 3, 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 telles informations devraient être mises à disposition, en particulier, lorsque l'autorité de contrôle est saisie par la personne concernée qui entend exercer les droits énoncés dans cet article, sous-réserve des exceptions prévues à l'article 9 paragraphe 1.

115. 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 traitées 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 prendre des mesures contre les responsables du traitement 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 le cas échéant les autorités compétentes.

116. Par ailleurs, aux termes du paragraphe 3, toute personne concernée 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. Outre ces investigations, en vertu des paragraphes 2(c) et 2(d), les autorités de contrôle peuvent notamment décider Les ressources nécessaires à l'exercice de leur mission doivent leur être allouées. 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.

117. 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. Ce pouvoir

[18] Voir note de bas de page 17.

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.

118. Lorsqu'une décision administrative produit des effets juridiques, la personne concernée est en droit de disposer d'un recours juridictionnel effectif conformément au droit interne applicable.

119. Le paragraphe 2(e) traite du rôle des autorités de contrôle en matière de sensibilisation. 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 125) ; elle pourra également publier des avis, émettre des recommandations générales relatives à la bonne application des règles de protection des données ou utiliser tout autre moyen de communication. 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.

120. Comme prévu au paragraphe 2bis, les autorités de contrôle peuvent, conformément au droit applicable, 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.

121. L'autorité pourrait, outre le pouvoir consultatif prévu au paragraphe 2bis, 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.

122. L'article 12bis ne fait pas obstacle à l'attribution d'autres pouvoirs aux autorités de contrôle.

123. 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, notamment : 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 aux réunions pertinentes sans restrictions injustifiées, la possibilité de consulter des experts techniques ou autres ou d'organiser des consultations externes, la disponibilité de ressources suffisantes, la possibilité de recruter ses propres agents ou encore l'adoption de décisions sans influence, qu'elle soit directe ou indirecte.

124. 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 dans les cas où elles l'estiment nécessaire, pour autant qu'elles portent un jugement indépendant.

125. 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.

126. Nonobstant 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.

127. 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 peut pas faire obstacle à la possibilité pour tout individu concerné d'exercer un recours juridictionnel (voir paragraphe 118).

128. En vertu du paragraphe 7 les autorités de contrôle sont tenues de coopérer entre elles. La coopération peut prendre plusieurs formes ; 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, et des formes plus « souples » comme la sensibilisation, la formation ou l'échange de personnel (voir les « actions conjointes » à l'article 12bis.7.b).

129. 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 : « 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 les informations confidentielles, y compris des données à caractère personnel.

130. Les données à caractère personnel ne peuvent faire l'objet d'un échange qu'à la condition : qu'elles soient essentielles à la coopération (c'est à dire que la coopération deviendrait inopérante sans ces informations) ou 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 (voir également l'article 16.b concernant les motifs de refus).

131. 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.

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

133. 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 n'exclut pas la possibilité, pour les autorités de contrôle des Parties, de s'associer à d'autres réseaux.

134. 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 indépendants dans l'exercice de leurs fonctions juridictionnelles. Une telle dérogation devrait être strictement limitée aux activités judiciaires proprement dites conformément au droit interne.

## Chapitre IV – Entraide

### Article 13 – Coopération entre les Parties

135. Le chapitre IV (articles 13 à 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. L'entraide est obligatoire, à l'exception des cas prévus à l'article 16. En vertu de l'article 13, 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.

136. 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, il ne peut être exclu qu'une Partie désigne une autre autorité pour donner effet aux dispositions de l'article 13.

137. 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**

138. 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 indépendamment de son lieu de résidence ou sa nationalité.

139. Aux termes du paragraphe 2, lorsque la personne concernée réside dans une autre Partie, 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.

140. Les personnes qui résident à l'étranger peuvent par ailleurs disposer de la possibilité d'exercer leurs droits avec l'aide des agents diplomatiques ou consulaires de leur propre pays.

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

**Article 15 – Garanties concernant l'assistance**

142. 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 de protection des données d'autres Parties et des personnes concernées résidant à l'étranger.

143. 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**

144. 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.

145. 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. Par ailleurs, l'autorité saisie peut être tenue par le droit applicable de veiller au respect d'autres intérêts d'ordre public (par exemple le fait d'assurer la confidentialité d'une enquête de police). L'autorité de contrôle peut à ce titre être obligée d'omettre certaines informations ou certains documents de sa réponse à une demande d'assistance.

**Article 17 – Frais et procédures de l'assistance**

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

147. 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

148. 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.

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

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

151. 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).

152. 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).

153. 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. 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, à la demande de cet Etat ou organisation internationale (article 19, lettre f).

154. 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.

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

156. 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

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

158. 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).

159. 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

160. 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

161. 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 Etat 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.

162. 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 soumises au droit public international.

### Article 24 – Clause territoriale

163. 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

164. 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 exceptions et restrictions admises par certains articles.

### Article 26 – Dénonciation

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

### Article 27 – Notification

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