EXPOSÉ DES MOTIFS

Recommandation Rec (2002) 9
du Comité des Ministres aux Etats membres
sur la protection des données à caractère personnel
collectées et traitées à des fins d'assurance

(adoptée par le Comité des Ministres le 18 septembre 2002
lors de la 808e réunion des Délégués des Ministres)

Avant-propos

Le Conseil de l'Europe est une organisation politique qui a été créée le 5 mai 1949 par dix Etats européens dans le but de réaliser une union plus étroite entre ses membres. Il compte aujourd'hui quarante-quatre Etats membres[1].

Les principaux objectifs de l'Organisation sont de promouvoir la démocratie, les droits de l'homme et la prééminence du droit, ainsi que de rechercher des solutions communes aux problèmes politiques, sociaux, culturels et juridiques de ses Etats membres. Depuis 1989, elle a intégré la plupart des pays d'Europe centrale et orientale, et les soutient dans leurs efforts en vue de mettre en oeuvre et de consolider leurs réformes politiques, législatives et administratives.

Les travaux du Conseil de l'Europe ont débouché sur l'adoption, à ce jour, de plus de 178 conventions et accords européens, qui constituent la base d'un «espace juridique commun» en Europe. De nombreuses recommandations du Comité des Ministres proposent des principes d'action aux gouvernements nationaux.

Le siège permanent du Conseil de l'Europe est à Strasbourg (France). Le statut de l'Organisation prévoit deux organes constitutifs : le Comité des Ministres, composé des ministres des Affaires étrangères des quarante-quatre Etats membres, et l'Assemblée parlementaire, formée de délégations des quarante-quatre parlements nationaux. Le Congrès des pouvoirs locaux et régionaux de l'Europe représente les collectivités territoriales dans les Etats membres.

La Cour européenne des Droits de l'Homme est l'instance judiciaire compétente pour statuer sur les requêtes introduites contre un Etat par des particuliers, des associations ou d'autres Etats contractants pour violation de la Convention européenne des Droits de l'Homme.

Mission et action du Conseil de l'Europe dans le domaine de la protection des données

1. Quarante-quatre Etats membres à la date de la publication: Albanie, Andorre, Arménie, Autriche, Azerbaïdjan, Belgique, Bosnie-Herzégovine, Bulgarie, Croatie, Chypre, République tchèque, Danemark, Estonie, Finlande, France, Géorgie, Allemagne, Grèce, Hongrie, Islande, Irlande, Italie, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Moldova, Pays-Bas, Norvège, Pologne, Portugal, Roumanie, Fédération de Russie, Saint-Marin, Slovaquie, Slovénie, Espagne, Suède, Suisse, « l'ex-République yougoslave de Macédoine », Turquie, Ukraine, Royaume-Uni.

Une des premières conventions établies par le Conseil de l'Europe, qui est aussi l'une des plus importantes - elle est prévue par l'article 1 du Statut du Conseil de l'Europe - est la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, ouverte à la signature en 1950. Cette Convention est caractéristique de la spécificité européenne en matière de défense des droits de l'homme, du fait notamment que les Etats qui l'ont ratifiée et ont reconnu la juridiction obligatoire de la Cour doivent se plier aux arrêts de la Cour européenne des Droits de l'Homme qui les concerne.

Plusieurs dispositions de cette Convention sont pertinentes « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel » et, notamment, les articles 8 et 10. Inversement, la protection des données vise à préciser la portée de certaines dispositions de la Convention et des relations entre ces dispositions.

Selon l'article 8 de cette Convention, « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Il ne peut y avoir d'ingérence d'une autorité publique dans l'exercice de ce droit que si cette ingérence est prévue par la loi et constitue une mesure qui, dans une société démocratique, est nécessaire à la défense d'un certain nombre de buts légitimes, limitativement énumérés. Mais, dans son article 10, la Convention affirme également le droit fondamental à la liberté d'expression. Ce droit inclut explicitement « la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence des autorités publiques et sans considération de frontières ».

Dans la logique de la Convention, les articles 8 et 10 ne sont pas contradictoires, mais complémentaires. Toutefois, dans la pratique, la jouissance de l'un de ces droits se trouve parfois limitée par l'autre droit. C'est pourquoi, dans leur jurisprudence, les organes de la Convention européenne des Droits de l'Homme définissent les limites de l'exercice de chacun de ces droits. En particulier, ils précisent la mesure dans laquelle les autorités publiques sont en droit d'interférer dans les droits reconnus par la Convention ou incités à assortir de garanties légales des secteurs particuliers. La Cour a ainsi jugé que « la protection des données constitue un élément fondamental de la protection effective du droit au respect de la vie privée ».[2] Cette jurisprudence relève d'un grand intérêt pour la poursuite des travaux du Conseil de l'Europe dans le domaine de la protection des données. Elle demeure également pour les gouvernements une source importante de critères d'élaboration de règles nationales dans ce domaine. Dans les années qui ont suivi l'adoption de la Convention européenne des Droits de l'Homme, il est apparu que, pour être efficace, la protection juridique de la vie privée devait être développée de manière plus spécifique et systématique.

Dès le début des années 60, les progrès rapides réalisés dans le domaine du traitement électronique des données et l'apparition des premiers ordinateurs ont permis aux administrations publiques et aux grandes entreprises de constituer d'importantes banques de données, d'améliorer et d'accroître la collecte, le traitement et l'interconnexion des données à caractère personnel. Si cette évolution a présenté de grands avantages du point de vue de l'efficacité et de la productivité, elle s'est en revanche traduite par une tendance à l'enregistrement électronique de données sans garanties suffisantes. Face à cette tendance et

2. *Z. c. Finlande*, arrêt du 25 février 1997, Rec. 1997. Jurisprudence confirmée dans les arrêts *M.S c. Suède,* du 27 août 1997, Rec. 1997, *Amann c. Suisse,* du 16 février 2000, Rec. 2000, et *Rotaru c. Roumanie,* du 4 mai 2000, Rec. 2000.

avec l'impulsion de l'Assemblée parlementaire, le Conseil de l'Europe a décidé d'établir un cadre de principes et de normes spécifiques afin d'éviter la collecte et le traitement déloyaux de données à caractère personnel, destiné tant au secteur public qu'au secteur privé.

Un premier pas a été fait dans cette direction en 1973 et 1974 avec l'adoption des Résolutions (73) 22 et (74) 29, qui ont défini les principes de la protection des données à caractère personnel dans les traitements automatiques de banques de données dans les secteurs privé et public. L'objectif était de favoriser l'élaboration de législations nationales inspirées de ces résolutions. Lors de l'élaboration de ces textes, il a été admis qu'une protection générale des données à caractère personnel ne serait efficace que si l'on renforçait encore les règles nationales et la coopération internationale au moyen de normes internationales à caractère contraignant. La même suggestion a été faite lors de la Conférence européenne des ministres de la Justice, en 1972.

Ainsi, le 28 janvier 1981, la Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel (STE n° 108), que l'on nomme « Convention 108 »,[3] a été ouverte à la signature. Ce texte constitue le premier instrument international juridiquement contraignant dans le domaine de la protection des données. Selon cette Convention, les Parties prennent, dans leur droit interne, les mesures nécessaires pour donner effet aux principes qu'elle pose afin de garantir sur leur territoire le respect des droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel. Ces principes portent notamment sur la qualité des données, à savoir :

– le caractère licite et loyal de la collecte et du traitement automatisés des données ;
– l'enregistrement des données pour des finalités déterminées et légitimes ;
– leur non-utilisation à des fins incompatibles avec ces finalités ;
– leur conservation dans les limites de ce qui est nécessaire pour ces finalités;
– le caractère adéquat, pertinent et non excessif (proportionnalité) des données enregistrées par rapport aux finalités, ou encore
– leur exactitude.

Ils portent également sur :

– l'interdiction du traitement automatisé de données sensibles (opinions politiques, croyances religieuses, race, condamnations pénales, données médicales, etc.), sauf garanties appropriées ;
– l'information des personnes concernées ;
– les droits d'accès et de rectification.

La Convention 108 prévoit, en outre, la libre circulation des données à caractère personnel entre les Etats parties à la Convention. Cette libre circulation ne saurait être restreinte pour des raisons de protection des données à caractère personnel. Les Parties peuvent néanmoins déroger à cette disposition lorsque :

- la protection des données à caractère personnel dans l'autre Partie n'est pas « équivalente » ou

3. Il est fait référence ci-dessous à « la Convention 108 ».

- le transfert a lieu vers un Etat tiers, non partie à la Convention 108.

Le protocole additionnel à la Convention 108, adopté le 23 mai 2001, prévoit, en outre, l'obligation pour les Parties de se doter d'une ou de plusieurs autorités exerçant un contrôle en toute indépendance, ainsi que l'obligation de ne pas permettre, en principe, le flux des données à destination de pays ou d'organisations n'offrant pas un niveau de protection adéquat.

La Convention 108 met en place un Comité consultatif, constitué de représentants des Parties à la Convention, qui est responsable de l'interprétation des dispositions, et qui veille à faciliter et à améliorer la mise en oeuvre de la Convention 108. C'est ce comité qui a pris l'initiative d'examiner dans quelle mesure l'utilisation de clauses contractuelles pouvait faciliter les flux de données entre les Parties à la Convention 108 et les Etats non contractants, et qui a élaboré, avec la Commission européenne et la Chambre Internationale de Commerce, un modèle type de clauses contractuelles.

L'article 4 de la Convention 108 prévoit que les Parties doivent prendre, dans leur droit interne, des mesures afin de donner effet aux principes de la protection des données énoncés dans la Convention 108 avant de pouvoir en devenir partie contractante. Vingt-huit Etats membres[4] ont à ce jour ratifié la Convention 108. D'autres Etats[5] l'ont signée, et certains d'entre eux ont adopté une loi sur la protection des données et préparent la ratification de la Convention 108. Plusieurs Etats membres du Conseil de l'Europe insèrent la protection des données dans le catalogue des droits fondamentaux de leur Constitution. En outre, l'article 23 de la Convention prévoit que tout Etat non membre du Conseil de l'Europe peut adhérer à la Convention. Le 15 juin 1999, les Délégués des Ministres du Conseil de l'Europe ont adopté un amendement à la Convention 108 permettant l'adhésion des Communautés européennes. Cet amendement entrera en vigueur 30 jours après que toutes les Parties l'auront accepté.

Depuis l'adoption de la Convention 108, en 1981, la société s'est informatisée à un point tel que l'utilisation de l'ordinateur individuel et des réseaux électroniques est devenue courante, permettant ainsi à toute personne ou organisation de procéder au «traitement automatisé des données». Dans l'intervalle, le développement socio-économique s'est traduit par des formes encore plus complexes d'organisation, de gestion et de production qui reposent sur de puissants systèmes de traitement. Dans ces conditions, le particulier devient à n'en pas douter un agent actif de la «société de l'information» qui, à son tour, risque de plus en plus de porter atteinte à sa vie privée par l'intermédiaire des systèmes d'information de nombreux services privés et publics tels que les banques, les organismes de crédit, la sécurité sociale, les assurances, la police ou les soins médicaux.

Cette évolution constitue un défi considérable du point de vue de la protection des données. L'adoption par le Comité des Ministres, le 7 mai 1999, de la Déclaration relative à une politique européenne pour les nouvelles technologies de l'information, évoquant la protection des données, reflète la nécessité de rechercher des solutions communes aux problèmes posés par le développement de ces technologies.

---

4. Autriche, Belgique, Chypre, Danemark, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Islande, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Pays-Bas, Norvège, Pologne, Portugal, République Tchèque, Roumanie, Slovaquie, Slovénie, Espagne, Suède, Suisse et Royaume-Uni.

5. Bulgarie, Fédération de Russie, Géorgie, Moldova et Turquie.

Aujourd'hui, un nombre sans cesse croissant de nouveaux problèmes et de questions pratiques est soumis aux autorités nationales chargées de la protection des données ou, dans la plupart des pays, à des commissaires à la protection des données.[6] Ces autorités sont devenues une partie intégrante du système de contrôle dans une société démocratique. Elles doivent interpréter leur droit interne en fonction des principes de la Convention 108 et les appliquer à ces nouveaux problèmes et questions. Le développement de la jurisprudence dans le domaine de la protection des données contribue à donner des solutions spécifiques à des problèmes particuliers qui se posent de manière différente suivant les secteurs considérés.

Les principes généraux de la protection des données nécessitent d'être précisés davantage dans la pratique. En effet, les dispositions de la Convention 108 et les nécessaires législations générales sur la protection des données au niveau du droit interne ne peuvent réglementer précisément toutes les situations où des données à caractère personnel sont collectées et traitées. Des règles spécifiques sont nécessaires suivant les secteurs : médical, sécurité sociale, assurance, banque, emploi, police, télécommunications, marketing direct, etc. Dans chacun de ces secteurs, les données doivent être collectées et traitées en conformité avec les principes fondamentaux de la Convention 108, mais les moyens d'y parvenir peuvent être différents. Dans certains secteurs, les conditions peuvent être plus souples que dans d'autres et l'autorégulation peut être plus développée dans une profession que dans une autre.

Sur la base de la Convention 108, le Conseil de l'Europe a adopté plusieurs recommandations sectorielles. Ces recommandations du Comité des Ministres s'adressent aux gouvernements de l'ensemble des Etats membres du Conseil de l'Europe. Bien qu'elles ne soient pas juridiquement contraignantes, elles constituent des normes de référence, et contiennent une invitation à considérer de bonne foi la possibilité d'élaborer et d'appliquer le droit interne conformément à l'interprétation convenue au niveau international des principes énoncés dans la convention et la recommandation.

Afin d'établir ces différentes recommandations, le Comité des Ministres a mis en place, en 1976, un Comité d'experts sur la protection des données, devenu ultérieurement le Groupe de projet sur la protection des données (CJ-PD). Ce comité est composé d'experts au titre de chacun des quarante-quatre Etats membres qui, dans leur pays respectif, ont une responsabilité en matière de protection des données. Pour certaines questions, ces experts sont parfois accompagnés de consultants spécialisés dans le domaine concerné. De plus, il est de tradition dans la politique du Conseil de l'Europe d'inviter à de telles réunions intergouvernementales des observateurs des organisations professionnelles européennes d'employeurs et d'employés et des associations non gouvernementales travaillant sur le sujet concerné. La Commission européenne participe également à l'élaboration de ces recommandations dans le domaine de ses compétences, notamment sur la base de la Directive 95/46/CE du Parlement européen et du Conseil, et sur la protection de l'individu à l'égard du traitement automatisé des données à caractère personnel et sur la libre circulation de ces données.

6. Depuis 1989, le Conseil de l'Europe élit son propre commissaire à la protection des données, qui supervise la protection des données à caractère personnel au Secrétariat Général.

Au fil des années, le Groupe de projet n'a pas seulement élaboré une série de recommandations,[7] mais il a également publié des études sur des sujets ponctuels dans le domaine de la protection des données[8].

7. 1. Recommandation n° R (99) 5 sur la protection de la vie privée sur Internet (23 février 1999),
   2. Recommandation n° R (97) 18 sur la protection des données à caractère personnel collectées et traitées à des fins statistiques (30 septembre 1997),
   3. Recommandation n° R (97) 5 sur la protection des données médicales (13 février 1997),
   4. Recommandation n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunications, eu égard notamment aux services téléphoniques (7 février 1995),
   5. Recommandation n° R (91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics (9 septembre 1991),
   6. Recommandation n° R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes (13 septembre 1990),
   7. Recommandation n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi (18 janvier 1989),
   8. Recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (17 septembre 1987),
   9. Recommandation n° R (86) 1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale (23 janvier 1986),
   10. Recommandation n° R (85) 20 relative à la protection des données à caractère personnel utilisées à des fins de marketing direct (25 octobre 1985),
   11. Recommandation n° R (83) 10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques (23 septembre 1983), remplacée par la Recommandation n° R (97) 18, citée ci-dessus en ce qui concerne les finalités statistiques,
   12. Recommandation n° R (81) 1 relative à la réglementation applicable aux banques de données médicales automatisées (23 janvier 1981), remplacée par la Recommandation R (97) 5 citée ci-dessus.

8. « Les nouvelles technologies: un défi pour la vie privée? » (1989),
« La protection des données et les médias » (1990),
« Les numéros personnels d'identification: leur mise en œuvre, leur utilisation et la protection des données » (1991).

INTRODUCTION

A. Les enjeux

1. L'informatisation croissante des activités et les développements technologiques incessants influencent nécessairement les sociétés contemporaines et les rapports des individus. L'échange et le traitement instantanés d'informations considérables constituent un intérêt tant pour l'individu que pour les divers agents économiques, y compris dans le secteur des assurances.

2. En même temps, les risques inhérents à ces progrès doivent être attentivement considérés au regard des droits de l'homme et des libertés fondamentales, notamment du droit au respect de la vie privée.

3. Le secteur de l'assurance attache la plus grande importance au respect de la vie privée et à la sécurité. Ces préoccupations sont partagées par les clients ou clients potentiels, c'est-à-dire les personnes concernées par d'éventuels traitements de leurs données. Ces personnes considèrent la confidentialité de leurs rapports comme un élément déterminant de leurs choix.

4. Cette recommandation vise essentiellement à assurer l'équilibre entre, d'une part, les intérêts des compagnies d'assurance et le fonctionnement des entreprises et, d'autre part, la protection de la vie privée.

5. Les assureurs légitiment la collecte et le traitement des données d'assurance notamment par le souci de garantir une sélection adéquate et une tarification correcte des risques liés à leur profession. Une meilleure appréciation des risques leur permet d'exercer leurs activités selon les besoins des consommateurs. Ces activités seraient inévitablement entravées par un défaut d'information. Le traitement remplit aussi un rôle important dans la lutte contre les fraudes : le transfert et l'échange de données sont nécessaires aux compagnies d'assurance pour déjouer les fraudes, préjudiciables aux autres assurés.

6. Ainsi, les assureurs sont amenés à traiter des données à caractère personnel dans le cadre médical, par exemple, de l'assurance-vie ou de l'assurance-maladie.

7. La collecte et le traitement à des fins d'assurance de données à caractère personnel requièrent une supervision afin de prévenir tout usage déloyal ou illicite de ces données. Cette supervision doit porter également sur les transferts de ces données par-delà les frontières, vers des pays ne disposant pas d'un niveau satisfaisant de protection. Il s'agit en particulier d'éviter que des données collectées et traitées à des fins déterminées et légitimes soient utilisées à des fins autres que celles initialement prévues. En particulier, il convient d'éviter des traitements débouchant sur des actes discriminatoires envers des assurés ou des catégories d'assurés.

8. L'élaboration de principes spécifiques pour le secteur de l'assurance dans le cadre de cette recommandation a pour objectif de répondre à toutes ces préoccupations.

9. La recommandation s'applique à l'ensemble des agents économiques qui mènent une activité d'assurance, qu'il s'agisse ou non d'une compagnie d'assurance ou de courtage, mais

ne s'applique pas à la sécurité sociale, à moins qu'un Etat décide d'étendre à la sécurité sociale le champ d'application de leur droit interne mettant en oeuvre cette recommandation.

B. Caractéristiques de l'assurance

10. L'assurance est le moyen de limiter les conséquences négatives de l'incertitude. Ainsi, au travers d'une société d'assurance, les individus ou les entreprises échangent des risques entre eux, les mutualisent, de façon non pas à supprimer l'incertitude, mais à minorer ses effets négatifs. Le concept même de l'assurance est à la fois profondément individuel - l'assuré cherche à se protéger contre les conséquences négatives de la survenance de tel ou tel événement défavorable - et profondément collectif - en se protégeant chacun protège aussi les autres. En réduisant les conséquences négatives de l'occurrence des risques sur le patrimoine physique (assurance dommages) et sur le patrimoine humain (assurance-vie) ; l'assurance parvient à être un puissant « générateur de sécurité », propice à la poursuite et à l'essor des activités économiques et sociales, au bon déroulement des contrats de toute nature, à la réduction des disparités issues nécessairement du règne généralisé de l'aléa.

11. L'assurance est une opération organisée, comportant à la fois certains éléments spécifiques et certaines règles techniques. Selon une définition classique quatre éléments interfèrent :

a. le risque : événement futur, incertain et ne dépendant pas de la volonté de l'assuré ou événement certain, mais dont la date de survenance est inconnue ;

b. la prime : cotisation que verse l'assuré à l'assureur en échange de la garantie qui lui est accordée ;

c. la prestation de l'assureur : en cas de réalisation d'un risque, l'assureur verse une prestation ;

d. la compensation au sein de la mutualité : chaque souscripteur verse sa prime sans savoir si c'est lui ou un autre qui en bénéficiera, mais conscient du fait que c'est grâce à ses versements et à ceux des autres souscripteurs que l'assureur pourra indemniser ceux qui auront été sinistrés. L'ensemble des personnes assurées contre un même risque et qui cotisent mutuellement pour faire face à ses conséquences constitue une mutualité. L'assureur est donc l'organisation de la solidarité entre les gens assurés contre la survenance d'un même événement.

12. Pour calculer le risque, l'assurance utilise ses méthodes statistiques. Ces méthodes sont principalement basées sur la loi des grands nombres (si on possède des études portant sur un très grand nombre de cas, on connaît de manière suffisamment précise la probabilité de survenance d'un événement) et sur les données statistiques des sinistres, qui sont indispensables à l'assurance. Elles permettent de connaître la fréquence des risques à assurer et les coûts moyens des sinistres.

13. La nature des activités de l'assureur, gestionnaire de la masse des primes de la mutualité, implique que des sommes considérables sont mises de côté, sous forme de provisions, pour faire face aux engagements futurs. Ces provisions, sévèrement réglementées

pour protéger les assurés, se traduisent par des investissements importants pour les économies nationales.

C. Evolution normative en matière de protection des données

14. Le législateur et, parfois, dans certains pays, les professionnels de l'assurance ont élaboré des normes de protection des données dans le domaine des assurances ou fixé des garanties. Dans plusieurs pays, des codes de déontologie ont ainsi été adoptés. Parfois, des règles sectorielles spécifiques réglementent ou interdisent la collecte et l'utilisation de certaines données, telles que les données génétiques qui sont susceptibles de faire apparaître les caractéristiques héréditaires d'une personne ou d'une lignée.

15. Les législations de protection des données ont pour objectif de garantir les droits fondamentaux des personnes et, en particulier, de leur vie privée. Les professionnels de l'assurance sont tenus à des règles de confidentialité qui poursuivent, en partie, des objectifs similaires, et les règles ou pratiques qu'ils élaborent sont nécessaires et complètent les législations nationales. L'activité d'assurance ne peut en effet se développer sans un cadre juridique approprié. L'autoréglementation et le recours à des techniques appropriées en sont le complément.

D. Historique de la recommandation

16. En novembre 1990, le Groupe de projet sur la protection des données a donc estimé qu'il fallait « examiner les problèmes de protection des données posés par la collecte et le traitement des données à caractère personnel au sein du secteur de l'assurance en vue de rédiger un instrument juridique approprié ».

17. Le groupe de travail n° 14 a été établi à cette fin. Il a été présidé par le Dr J. A. Cannataci (Malte) et était composé d'experts au titre de l'Allemagne, de Malte, de la Norvège, de l'Espagne, de la Suède, de la Suisse et du Royaume Uni. Il s'est réuni six fois entre février 1994 et octobre 1996. Des experts au titre de l'Albanie, l'Autriche, le Bélarus, la Belgique, la Bulgarie, le Canada, la Croatie, la Hongrie, le Luxembourg, les Pays-Bas, la Russie, « l'ex-République yougoslave de Macédoine », ainsi que des représentants de la Chambre Internationale de Commerce, du Comité Européen des Assurances et du Bureau International pour la Production de Police d'Assurance et pour la Réassurance ont participé aux réunions.

18. La Commission européenne a participé à l'élaboration de la recommandation dans le domaine de ses compétences et sur la base, notamment, des dispositions de la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 sur la protection des individus à l'égard du traitement des données à caractère personnel et de la libre circulation de ces données.

19. Le projet de recommandation sur la protection des données à caractère personnel, collectées et traitées à des fins d'assurance a été approuvé par le Groupe de projet sur la protection des données lors de sa 37^{e} réunion, du 12 au 15 octobre 1999, et par le Comité européen de coopération juridique le 31 mai 2001.

20. Le 18 septembre 2002, le Comité des Ministres a adopté la Recommandation N° R (2002) 9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance, et autorisé la publication du présent « Exposé des motifs ».

Commentaires sur les dispositions de la recommandation

A. Préambule

21. Dans le préambule sont énoncées les considérations qui ont amené le Comité des Ministres à adresser la recommandation aux gouvernements des Etats membres.

a. Parmi ces considérations, le Comité des Ministres rappelle l'importance qu'il y a, dans le domaine de l'assurance, à promouvoir et à garantir la protection des données à caractère personnel et, notamment, la protection des données sensibles, ainsi que le prévoit l'article 6 de la Convention 108.

b. Le Comité des Ministres reconnaît la nécessité qu'il y a à traiter une quantité considérable de données à caractère personnel par des moyens automatisés, pour permettre une gestion rationnelle et économique de l'assurance dans un secteur fortement concurrentiel, et pour lutter contre la fraude.

c. Le Comité des Ministres observe également que la fourniture d'une assurance, parmi les diverses branches de l'assurance et les différentes catégories de contrats, n'est pas du seul ressort des compagnies d'assurance. Les intermédiaires de l'assurance exercent dans ce secteur une activité déterminante. Enfin, l'Etat intervient également dans le secteur de l'assurance, en ce qu'il réglemente le secteur des assurances. De plus, certaines autorités ou organismes publics ou investis de missions publiques offrent parfois eux-mêmes des assurances.

d. Le Comité des Ministres observe les nombreuses situations dans lesquelles le recours à un contrat d'assurance s'est généralisé ou est devenu indispensable, qu'il s'agisse d'une obligation légale, par exemple l'assurance automobile, ou d'une pratique généralement acceptée. De ce fait, les individus sont conduits à fournir de nombreux renseignements inhérents à leur vie privée et, en particulier, des données sensibles qui font ensuite l'objet de divers traitements à des fins d'assurance.

e. Le Comité des Ministres reconnaît l'importance que revêtent, dans le domaine de l'assurance notamment, la qualité des données collectées et traitées, conformément à l'article 5 de la Convention 108 et, en particulier, la pertinence, l'intégrité, la disponibilité, mais aussi la confidentialité qui est inhérente au rapport de confiance qui s'instaure entre l'assureur et l'assuré, à l'instar du secteur des banques et des institutions financières.

f. Le Comité des Ministres définit comme objectif de la recommandation l'établissement de procédures appropriées en vue de garantir que la collecte et le traitement des données à caractère personnel à des fins d'assurance respectent les droits et libertés fondamentales des individus, et assurent un équilibre approprié entre la libre circulation de l'information et le droit au respect de la vie privée. Une telle réglementation est rendue nécessaire dans un contexte de mobilité des

individus et de mondialisation des marchés et activités commerciales, nécessitant un échange d'informations transfrontières et une protection équivalente dans tous les Etats membres du Conseil de l'Europe.

B. Dispositif de la recommandation

22. Le Comité des Ministres recommande d'abord aux gouvernements des Etats membres de prendre des mesures pour que les principes contenus dans l'annexe soient reflétés dans leur droit et leur pratique. Le libellé de cette recommandation s'adresse également aux Etats membres non encore Parties à la Convention 108 et qui, par conséquent, n'ont pas pris, dans leur droit interne, toutes les mesures nécessaires pour donner effet aux principes de base de protection des données.

23. Deuxièmement, les gouvernements sont encouragés à diffuser largement le contenu de l'annexe à la recommandation auprès des autorités nationales compétentes en matière de protection des données et de toutes les personnes qui, de par leur profession, sont appelées à collecter et à traiter des données à caractère personnel à des fins d'assurance ou à veiller sur la protection de telles données.

24. Troisièmement, les gouvernements sont invités, le cas échéant, à promouvoir dans le secteur des assurances des dispositions législatives et à encourager l'établissement de règles de déontologie s'inspirant des principes de la présente recommandation.

Annexe à la recommandation

1. Définitions

25. **Le chapitre 1** établit les définitions de certains concepts centraux de la recommandation. Les expressions « droit interne », « loi », « prévu par le droit interne », « autorisé par le droit interne » ont été définies dans le cadre de la Recommandation n° R (97) 18 sur la protection des données à caractère personnel collectées et traitées à des fins statistiques (paragraphe 50 de l'exposé des motifs), conformément à la jurisprudence de la Cour européenne des Droits de l'Homme.

26. **Données à caractère personnel.** La définition est conforme à celle de la Convention 108, telle qu'interprétée dans le rapport explicatif de celle-ci. Elle a déjà été utilisée dans nombre de recommandations sectorielles spécifiques adoptées par le Comité des Ministres dans le domaine de la protection des données.

a. Personne: La définition se réfère à une personne physique. Toutefois, à l'égard des Parties qui étendent l'application de la Convention 108 (en vertu de son article 3, paragraphe 2.*b*) ou de la recommandation aux personnes morales (en vertu de son principe 2.4), la définition s'entend comme couvrant également celles-ci. Par ailleurs, les informations relatives à une personne physique peuvent se rapporter à une entité**,** par exemple à une entreprise unipersonnelle, constituant en même temps des données à caractère personnel (relatives au propriétaire, par exemple). Dans ce cas, elles relèvent de l'application de la recommandation.

b. Personne identifiable: une personne est dite « identifiable » lorsqu'elle peut être identifiée par des traitements ou recoupements de ses données à caractère personnel, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Une personne n'est pas « identifiable » si l'identification exige des activités déraisonnables, c'est-à-dire des opérations excessivement compliquées, longues et coûteuses. Ces conditions sont appréciées notamment en fonction des moyens techniques dont on peut disposer pour identifier les données pertinentes et dévoiler ainsi leur anonymat. De la sorte, compte tenu des progrès rapides des techniques et des méthodes informatiques, les coûts, délais et activités nécessaires à l'identification d'une personne, qui seraient aujourd'hui considérés comme « déraisonnables », pourraient ne plus l'être à l'avenir. Toutefois, la formulation actuelle est suffisamment flexible pour englober de tels développements.

27. **Données sensibles**. La définition repose notamment sur la liste minimale énoncée à l'article 6 de la Convention 108. Les poursuites pénales y ont été ajoutées, à l'instar de l'article 8 de la Directive 95/46/CE. Conformément à l'article 11 de la Convention 108, d'autres catégories de données à caractère personnel (telles que les données sur l'appartenance syndicale) peuvent être définies comme sensibles par le droit interne. Pour la définition des données médicales, il convient de se reporter à la Recommandation n° R (97) 5 relative à la protection des données médicales, y compris en ce qui concerne les données génétiques (voir son exposé des motifs, paragraphes 41 à 58).

28. **Fins d'assurance.** En l'absence de définition généralement reconnue sur le plan international, la définition « des fins d'assurance » se veut aussi large que possible. Cette définition met l'accent sur les finalités des traitements et non sur une délimitation arbitraire des différents secteurs concernés. Elle couvre toute opération de collecte et de traitement des données inhérente à l'activité d'assurance, liée, par exemple, à la couverture d'un risque, à la préparation, la conclusion, la mise en oeuvre et la cessation d'un contrat ou d'une police d'assurance. Elle couvre toute opération d'assurance quel que soit l'opérateur qui la réalise, qu'il s'agisse par exemple d'une compagnie d'assurance, d'un intermédiaire ou d'un organisme public. Elle couvre également les plans de retraite, mais ne couvre pas en revanche les jeux de hasard. Cette définition inclut aussi la sécurité sociale pour les Etats qui souhaiteraient faire usage de la faculté d'étendre le champ d'application du droit interne mettant en application cette recommandation à la sécurité sociale, conformément au Principe 2.5.

a. La « couverture » d'un risque se définit comme l'opération par laquelle l'assureur est tenu, moyennant rémunération sous forme de prime, de donner à l'assuré ou à un tiers une prestation en cas de réalisation d'un risque donné. Cette couverture peut résulter d'un contrat, d'une police ou de toute autre forme d'établissement d'une obligation juridique telle que les systèmes légaux de garantie contre les risques maladie, invalidité, vieillesse s'appliquant par exemple aux salariés du commerce et de l'industrie. Elle peut donc être établie à l'initiative d'une personne souhaitant contracter une assurance ou découler d'une disposition légale. En effet, dans la plupart des cas de couverture d'assurance, il y a un contrat, que l'assurance soit ou non obligatoire. Mais, dans certains pays, la couverture de l'assurance pour un immeuble, par exemple, peut s'apparenter à une décision administrative.

b. Le « risque », propre à l'activité d'assurance, dépend de la détermination, généralement entre l'assureur et son client, d'un aléa, d'un dommage ou de tout autre événement nécessaire ou susceptible d'advenir.

c. En outre, l'expression « toute opération » couvre la collecte et le traitement de données à caractère personnel effectués par un assureur pour la couverture d'un risque. Elle couvre également les opérations d'entremise d'assurance. Les intermédiaires de l'assurance, tels les courtiers, exercent une action déterminante dans ce secteur, notamment lors de la préparation du contrat ou de la réassurance. La finalité de l'activité du courtier est de trouver la meilleure couverture pour son client avec le paiement de la prime la moins élevée possible en contrepartie. En raison de cette finalité, le courtier transmet certaines données à caractère personnel à un certain nombre d'assureurs en vue de recevoir une offre. Cette expression couvre aussi les opérations réalisées par les experts dans leurs activités liées à l'assurance.

d. Conformément à l'article 5 de la Convention 108, les données à caractère personnel doivent être traitées uniquement pour des finalités déterminées. Elles ne doivent pas non plus être utilisées de manière incompatible avec ces finalités. Par conséquent, aux fins de cette recommandation, la détermination des « finalités d'assurance » est donc importante. C'est pourquoi, ces finalités et les finalités avec lesquelles elles peuvent être compatibles ont été spécifiées notamment au Principe 4.4 ou en relation avec les Principes 4.8, 8.1 et 13.1 de la recommandation. La finalité générale d'assurance doit donc être considérée à la lumière des définitions relatives à la couverture d'un risque et des finalités particulières spécifiées dans la recommandation.

29. **Traitement**. La définition se rapporte à l'ensemble des opérations automatisées nécessaires à l'activité d'assurance, à l'exception de la collecte lorsque celle-ci est réalisée sans que s'en suive un traitement automatisé. Le chapitre 2 spécifie la portée de ces opérations dans le champ d'application de la recommandation. Le choix d'appliquer cette recommandation aux traitements non automatisés relève des Etats membres.

30. **Communication**. Ce terme recouvre toute forme de mise à disposition des données à un tiers et, notamment, la transmission, la diffusion ou l'interconnexion. Il peut s'agir d'une mise à disposition active en réponse à une demande individuelle du tiers. Il peut également s'agir d'une mise à disposition passive par l'autorisation donnée au tiers d'avoir accès en ligne à des données à caractère personnel.

31. **Responsable du traitement**. Ce terme se réfère au concept de « maître du fichier » de l'article 2 de la Convention 108. Toutefois, la notion de « fichier » ne prend pas suffisamment en compte les développements technologiques du traitement des données à caractère personnel. A l'instar des recommandations précédentes, cette recommandation définit le concept de « responsable du traitement » qui s'applique à toute personne ou tout organisme qui détermine les finalités et les moyens de la collecte et du traitement des données à caractère personnel à des fins d'assurance. Ce concept est analogue à celui établi à l'article 2.*d* de la Directive 95/46/CE. Il appartient à chaque Etat membre de demander à tout responsable qui n'est pas établi à l'intérieur du pays de désigner un représentant qui garantira le respect des obligations prévues par la recommandation.

a. La définition couvre l'assureur, les organisations ou les personnes qui fournissent une assurance ainsi que les intermédiaires. Il convient d'observer que les courtiers d'assurance, les agents indépendants, mais aussi, le cas échéant, les experts ou les établissements financiers devraient être considérés, en principe, comme des responsables du traitement et non comme des sous-traitants, dès lors qu'ils collectent et traitent des données à caractère personnel, et ce même avant la conclusion d'un contrat. C'est au responsable du traitement qu'incombe le respect des principes en matière de protection de données, à l'exception des obligations particulières du sous-traitant éventuel en matière de sécurité.

b. La référence à l'autorité publique est incluse dans la définition car il y a, par exemple, des assurances contre les accidents du travail qui sont fournies par des autorités publiques. De même, dans l'assurance crédit caution, et autres aides à l'exportation, ce sont notamment des organismes publics qui délivrent des assurances, en particulier pour couvrir un risque politique.

32. **Sous-traitant :** Cette expression rend compte de l'activité spécifique des personnes spécialement mandatées pour réaliser une partie ou la totalité du traitement à la place et au nom du responsable du traitement. La responsabilité du sous-traitant diffère de celle du responsable du traitement du point de vue de la protection des données, conformément au chapitre 7 de la recommandation. Le concept de sous-traitant est analogue à celui établi à l'article 2.*e* de la Directive 95/46/CE.

2. Champ d'application

33. **Le Principe 2.1** circonscrit le champ d'application de la recommandation à « la collecte et au traitement des données à caractère personnel à des fins d'assurance ». La sécurité sociale est explicitement exclue du champ d'application de la recommandation compte tenu des régimes distincts auxquels sont soumis l'assurance privée, d'une part, et la sécurité sociale, d'autre part, dans le droit et la pratique de la plupart des Etats, et dans le droit international. Toutefois, compte tenu du fait que le droit interne et la pratique de certains Etats permettent d'assimiler la sécurité sociale à l'assurance du point de vue des règles applicables en matière de protection des données, le Principe 2.5 prévoit la possibilité pour les Etats d'étendre le champ d'application de cette recommandation à la sécurité sociale, ce qu'autorise la définition large qui a été adoptée des « fins d'assurance ». La recommandation couvre, entre autres, l'opération d'entremise d'assurance, par laquelle un courtier ou un agent sont amenés à traiter des données à caractère personnel. Le courtier ne conclut pas à proprement parler un contrat d'assurance ; s'il le fait, une compagnie d'assurance se réserve toujours un « droit d'acceptation ». Alors que le courtier est réputé agir pour le compte de l'assuré, l'agent quant à lui, agit en général en nom et place de l'assureur.

a. Dans le domaine de l'assurance, la collecte de données est souvent effectuée manuellement à l'aide de formulaires à remplir. Parfois ces fichiers manuels contiennent des données sensibles. Dès lors, la recommandation s'applique à toute collecte de données à caractère personnel à des fins d'assurance, que celle-ci soit effectuée par des moyens automatisés ou par des moyens manuels en vue d'un traitement automatisé ultérieur.

b. Le terme de traitement, tel qu'il est défini dans le Chapitre 1, recouvre une large variété d'opérations. La recommandation s'applique donc à toutes ces formes de traitement automatisé de données à caractère personnel.

34. **Le Principe 2.2** encourage les Etats membres à « étendre l'application de la présente recommandation aux traitements non automatisés des données à caractère personnel à des fins d'assurance ». En effet, l'article 3, paragraphe 2.*c* de la Convention 108 prévoit que les Parties peuvent étendre le champ d'application de celle-ci aux fichiers de données à caractère personnel ne faisant pas l'objet de traitements automatisés.

a. En pratique, la collecte de données est immédiatement suivie d'un traitement qui est souvent réalisé en partie automatiquement et en partie manuellement. Dans certains cas, les données à caractère personnel sont enregistrées ou conservées manuellement.

b. L'informatisation croissante des activités tend toutefois à diminuer le nombre et l'importance des fichiers manuels ;

c. On constate que, dans certains Etats membres, la législation sur la protection des données ne s'applique pas aux fichiers manuels. En revanche, d'autres pays ont déjà étendu le champ d'application de leur législation aux traitements non automatisés. Ainsi la Directive 95/46/CE s'applique aux fichiers manuels « structurés ».

d. Les Etats sont libres de déterminer l'ampleur et les modalités de cette extension. La recommandation encourage cette démarche afin de couvrir de tels fichiers, qui peuvent parfois contenir des données sensibles. Enfin, les Etats pourraient prévoir une période transitoire pour procéder à l'extension du champ d'application aux données à caractère personnel traitées manuellement à des fins d'assurance.

35. **Le Principe 2.3** précise que, dans aucun cas, des données ne devraient être traitées manuellement dans l'intention d'échapper aux principes de la présente recommandation. Cette disposition vise à prévenir des pratiques tendant à contourner les principes de protection des données lorsque les législations nationales ne s'appliquent pas aux traitements non automatisés.

36. **Le Principe 2.4** autorise une extension facultative du champ d'application de la recommandation à la protection des données relatives à des personnes morales et autres organisations, collectées et traitées à des fins d'assurances. Il s'agit, d'une part, d'assurer une protection efficace de la vie privée des personnes physiques et, d'autre part, de tenir compte de la faculté reconnue, par l'article 3.2.*b* de la Convention 108, aux Etats d'inclure dans le champ d'application de la recommandation, outre les personnes physiques, les groupements de personnes, associations, fondations, sociétés, corporations ou tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique.

37. Les données à caractère personnel collectées et traitées à des fins de sécurité sociale sont déjà régies par la Recommandation n° R (86) 1. Les systèmes de sécurité sociale des Etats membres sont très hétérogènes et il a été jugé opportun de circonscrire le champ d'application de la recommandation aux activités d'assurance et de laisser les gouvernements libres d'appliquer ou non ses dispositions au domaine de la sécurité sociale. Le principe 2.5 énonce ainsi une faculté supplémentaire pour les Etats qui le souhaitent d'étendre le champ d'application de cette recommandation à la collecte et au traitement de données à caractère personnel à des fins de sécurité sociale. Lorsque la faculté d'extension est utilisée, en principe, les dispositions de la

Recommandation n° R (86) 1 régissent la collecte et le traitement des données collectées et traitées à des fins de sécurité sociale, dans la mesure où la présente recommandation ne s'applique pas. Cela signifie qu'il ne peut y avoir d'insécurité juridique dans les cas où les assureurs fournissent une assurance sociale et privée ou dans le cadre des flux transfrontières de données entre Etats ayant des systèmes différents.

38. Cette faculté se justifie par le fait que certains Etats membres considèrent la sécurité sociale comme une branche de l'assurance, notamment du fait qu'une partie de la gestion de l'assurance sociale est confiée à des organismes privés ou semi-publics qui offrent également des prestations relevant de l'assurance privée. C'est notamment le cas de l'assurance-maladie, dont une partie relève de l'assurance sociale obligatoire et l'autre de l'assurance privée complémentaire. Dans un tel cas de figure, il peut se justifier de ne pas soumettre le traitement des données à caractère personnel à des régimes juridiques différents. Cette faculté permet également de tenir compte de l'évolution économique actuelle qui voit des pans entiers de la sécurité sociale traditionnellement aux mains d'organismes publics être privatisés. Elle tient compte de la difficulté à distinguer clairement secteur public et secteur privé, assurance et sécurité sociale: ainsi, dans certains pays, les accidents du travail relèvent du domaine public, mais c'est le secteur privé qui fait les contrats. Dans d'autres pays, des pans entiers du domaine des accidents du travail sont transférés au secteur privé. De même, ailleurs, une grande partie de l'assurance santé est confiée à l'assurance privée. Elle permet enfin de respecter les systèmes de sécurité sociale des Etats membres qui sont régis par des législations particulières échappant aux règles habituelles de l'assurance et qui suivent un régime de financement particulier. Dans ces cas, la Recommandation n° R (86) 1 s'applique à la collecte et au traitement de données à caractère personnel utilisées à des fins de sécurité sociale.

3. Respect de la vie privée

39. **Le Principe 3.1** rappelle l'objectif de la Convention 108 tel qu'il est énoncé à son article 1er: garantir à toute personne physique le respect de ses droits et de ses libertés fondamentales, et, notamment, de son droit à la vie privée, au regard du traitement automatisé de ses données à caractère personnel**.**

40. **Le Principe 3.2** dispose que les personnes impliquées dans une activité d'assurance et qui ont accès à des données à caractère personnel doivent être soumises à des règles de confidentialité prévues par des normes du droit interne et par la pratique, et qui peuvent éventuellement être complétées par des codes d'éthique agréés par les professionnels.

41. En outre, ce principe insiste sur le fait que les données médicales ne peuvent être collectées et traitées que par des professionnels des soins de santé ou par des personnes qui sont soumises à des obligations de confidentialité comparables ou d'efficacité égale, prévues par le droit interne.

4. Conditions générales régissant la collecte et le traitement des données à des fins d'assurance

42. **Le Principe 4.1** énonce quelques principes de base essentiels en ce qui concerne la protection des données. La recommandation rappelle que la communication au même titre que

l'interconnexion font partie de la définition du traitement et que des données à caractère personnel ne peuvent être communiquées que conformément aux dispositions de la recommandation et, notamment, du Chapitre 4. La communication des données à caractère personnel à d'autres fins que les fins d'assurance relève du Chapitre 8.

a. Par référence à l'article 5.*a* de la Convention 108, la recommandation réitère les principes suivant lesquels les données à caractère personnel doivent être obtenues et traitées loyalement et licitement. Le principe de la loyauté de la collecte et du traitement est explicité notamment au chapitre 5 sur l'information des personnes concernées en vue d'assurer la transparence des traitements à leur égard, mais concerne aussi les méthodes de collecte et de traitement. La licéité relève du Principe 4.3.

b. La recommandation dispose en outre, conformément à l'article 5.*b* de la Convention, que la collecte et le traitement des données à caractère personnel à des fins d'assurance ne peuvent avoir lieu que pour des finalités d'assurance déterminées et légitimes. La finalité, qui devrait être spécifique et explicite, relève du Principe 4.4 lorsqu'il s'agit d'une finalité d'assurance ou d'une finalité, en principe, compatible. Les Principes 4.8 (marketing direct), 8.1 (communication à d'autres fins que l'assurance) et 13.1 (conservation) couvrent les autres finalités. Toute finalité de traitement n'est pas en soi légitime car, même fondé sur une base de licéité donnée, un traitement peut conduire, par exemple, à des discriminations entre les personnes concernées.

c. Le deuxième paragraphe du Principe 4.1 illustre aussi l'application des principes de proportionnalité et d'exactitude qui se fondent sur l'article 5.*c* et *d* de la Convention : les données traitées doivent être adéquates, pertinentes et non excessives par rapport aux finalités poursuivies par le responsable du traitement, au moment de la collecte ou ultérieurement, et être exactes ; si nécessaire, elles doivent aussi être mises à jour. Dans le domaine de l'assurance, comme dans d'autres domaines ayant fait l'objet de recommandations spécifiques, le principe de proportionnalité implique que la collecte et le traitement des données à caractère personnel doivent être limités aux seules données nécessaires aux finalités d'assurance poursuivies, en fonction de la branche d'assurance considérée.

43. **Le Principe 4.2** dispose que les données à caractère personnel doivent être collectées en principe auprès de la personne concernée ou de son représentant légal. En pratique, la collecte des données n'est pas nécessairement effectuée auprès de la personne concernée, mais auprès d'un tiers, ce qui est pris en compte par le Principe 5.3 relatif à l'information des personnes concernées. Les données de la personne concernée peuvent être collectées auprès d'une autre personne du fait, par exemple, d'une disposition légale (Principe 4.3) ou en cas d'intermédiaires, de réassurance ou dans le but de détecter des fraudes (par exemple fraude à l'assurance-vie, fausse déclaration à l'assurance automobile). Lorsque ces données sont collectées dans une telle situation, la personne concernée doit aussi en être informée dans les conditions énoncées par la recommandation.

Licéité

44. L'article 5 de la Convention 108 exige que les données à caractère personnel soient obtenues de manière licite. Dans cette optique, la licéité de la collecte et du traitement de données à caractère personnel à des fins d'assurance doit reposer sur une base légale ou sur une base contractuelle ou sur le consentement des personnes concernées, ou encore sur la base d'un

intérêt légitime du responsable du traitement. Ces quatre conditions générales de licéité sont alternatives.

45. **Le Principe 4.3** porte sur l'application des conditions générales de licéité à différentes sortes de collectes et de traitements de données à caractère personnel à des fins d'assurance.

a. L'alinéa *a* concerne de façon spécifique des situations dans lesquelles la collecte et le traitement de données à caractère personnel à des fins d'assurance sont prévus par la loi. Une obligation de renseignement peut alors être imposée, directement aux personnes concernées, pour la souscription d'une assurance obligatoire en vertu de la loi (par exemple pour l'assurance d'un immeuble dans certains pays), ou indirectement, au responsable du traitement, lors d'une collecte effectuée en vertu du Principe 4.4.h. En ce qui concerne ce dernier cas, une compagnie d'assurance peut être amenée à collecter et traiter elle-même des données, par exemple aux fins de lutter contre le blanchiment de capitaux ou de combattre la criminalité organisée. La communication de ces données aux autorités publiques est régie par le Chapitre 8 de la recommandation.

b. Selon l'alinéa *b,* la collecte et le traitement de données à caractère personnel peuvent avoir également pour base juridique le contrat. Les éléments suivants ont été pris en considération:

– La référence à la « préparation » du contrat a été introduite dans le but de couvrir les mesures précontractuelles prises à la demande de la personne concernée. Cependant, la recommandation n'entend pas empêcher la prospection du marché par les compagnies d'assurance. Les compagnies d'assurance peuvent, de leur propre initiative, proposer à leur client de compléter un produit d'assurance. Par exemple, le fournisseur d'une assurance peut proposer de compléter une assurance hospitalisation par une assurance-vie. Lors de l'achat d'un billet de voyage, il peut être proposé de compléter une assurance liée à un bagage en cas de perte ou de vol par une assurance liée à la vie de la personne. Dans ces cas, les dispositions du principe 4.3.*d* peuvent aussi s'appliquer.

– La référence à « l'exécution » du contrat couvre les opérations réalisées par l'assureur liées à la mise en oeuvre et à la cessation du contrat.

– Enfin, la recommandation vise à protéger également les droits des personnes tierces à un contrat, mais qui ont un certain lien avec celui-ci. Il a ainsi été convenu que les données relatives au bénéficiaire du contrat d'assurance, non-partie au contrat, devraient être traitées sur la base offerte par le Principe 4.3.*d*, voire 4.3.*c*. Le but est de protéger de la façon plus adéquate les droits du bénéficiaire.

c. La licéité est en outre établie lorsqu'elle a pour fondement le consentement de la personne concernée, de son représentant légal ou de toute autorité établie par la loi, si le droit interne ne s'y oppose pas. Le consentement peut porter sur une seule ou plusieurs finalités d'assurance déterminées. Le responsable de traitement peut licitement demander un seul consentement pour plusieurs finalités. Les caractéristiques du consentement figurent au Chapitre 6 de la recommandation.

d. Enfin, la recommandation reconnaît la licéité d'une collecte et d'un traitement effectués en vertu d'un intérêt légitime poursuivi par le responsable du traitement. Par exemple, le responsable du traitement est habilité à collecter et traiter les données à caractère personnel du bénéficiaire d'une assurance-vie, non-partie au contrat, ou encore à proposer à un client de compléter sa couverture d'assurance. Toutefois, deux limites ont été fixées à l'usage de cette base juridique. En premier lieu, les données collectées par le responsable du traitement doivent être « nécessaires » à cet intérêt légitime. En second lieu, les intérêts de la personne concernée ne doivent pas prévaloir, le respect des Chapitres 3 et 4 devant être pleinement garanti. Dans ce contexte, une balance des intérêts en présence devra être effectuée.

Finalité

46. **Le Principe 4.4** est fondé sur une exigence de l'article 5 de la Convention 108, en vertu duquel les données à caractère personnel doivent uniquement être traitées pour des finalités déterminées et légitimes, et ne peuvent être utilisées à des fins incompatibles. Le premier paragraphe du Principe 4.4 énumère les finalités d'assurance. Le second paragraphe du Principe 4.4 rappelle le principe de « compatibilité ». Rédigé de manière souple, le Principe 4.4 permet de pouvoir prendre en compte l'évolution du secteur des assurances. Un traitement peut être réalisé pour une finalité, même incompatible avec la finalité de départ, si, par exemple, la loi le prévoit ou si la personne concernée y a malgré tout consenti, que ce soit ou non par contrat, et que le droit interne ne s'y oppose pas.

47. Les finalités des alinéas *a* à *k* couvrent les opérations réalisées par une compagnie d'assurance, par un établissement financier ou par un intermédiaire de l'assurance dès lors qu'ils poursuivent une finalité d'assurance.

a. Les finalités prévues aux alinéas *a* à *e* concernent les activités directement liées aux prestations d'une assurance. Ces activités nécessitent une collecte et un traitement de données à caractère personnel en vue de la préparation et de la fourniture d'un contrat, du paiement des primes et autres facturations, du règlement des demandes d'indemnisation ou d'autres prestations, de la réassurance ou de la coassurance.

b. Les finalités prévues aux alinéas *f* à *k* sont énoncées plutôt au regard des droits et des obligations du responsable du traitement, notamment:

– pour la prévention, la détection ou la poursuite des fraudes (4.4.*f*) en ce qui concerne les traitements effectués par les opérateurs de ce secteur, notamment les compagnies d'assurance. Dès lors qu'une communication est envisagée, il devrait exister un motif suffisant de soupçon avant que le responsable de traitement ne puisse procéder à un traitement spécifique, conformément au Chapitre 8 ;

– pour la contestation, l'exercice ou la défense d'un droit en justice (4.4.*g*);

– pour le respect d'une autre obligation légale ou contractuelle spécifique(4.4.*h*). Les obligations légales, autres que celles énoncées au 4.4.*g*, ont trait, notamment, au droit fiscal, à la sécurité sociale ou à la lutte contre la criminalité. De telles obligations peuvent également être de nature contractuelle. Par exemple, si les compagnies d'assurance utilisent d'autres fichiers que le registre de la clientèle à des fins de marketing direct, le

traitement doit rester possible pour éviter tout marketing direct envers des personnes concernées qui s'y sont opposées**.**

– pour la recherche de nouveaux marchés d'assurance (4.4.*i*). Cette finalité vise les cas où des recherches globales sont effectuées à l'aide de méthodes particulières d'opérations de traitement, en vue d'appréhender de nouveaux produits d'assurance conformément aux attentes latentes ou exprimées du marché. A cet égard, la Recommandation n° R (85) 20 relative à la protection des données à caractère personnel utilisées à des fins de marketing direct prévoit, notamment, que « sous réserve des limites prévues par le droit interne, toute personne devrait pouvoir collecter des données à caractère personnel à des fins de marketing direct à partir de fichiers accessibles au public ou d'autres publications" (voir le chapitre 2).

– pour la gestion interne d'une compagnie d'assurance (4.4.*j*). Peuvent être pris comme exemples : le calcul de provisions pour les salariés et l'information à l'intention des personnes concernées dans le but d'éviter les litiges d'assurance. Une autre raison provient du fait que les assureurs ont besoin d'analyser régulièrement la composition de leur portefeuille d'assurances. A partir d'une telle analyse, ils peuvent prendre des décisions en matière de gestion concernant les investissements liés à l'embauche des nouveaux collaborateurs et à la formation du personnel. Les assureurs concluent des contrats annuels avec des fournisseurs de soins de santé. Pour conclure de tels contrats, ils ont besoin de certaines informations qui nécessitent au préalable une analyse des données à caractère personnel collectées et traitées à des fins d'assurance ;

– pour l'activité d'actuariat (4.4.*k*). Le secteur de l'assurance est amené à utiliser l'actuariat ou la statistique qui par une synthèse d'informations individuelles, mettent en évidence les caractéristiques collectives d'une population déterminée. Ils permettent également aux assureurs de créer de nouveaux produits. Les traitements de données à caractère personnel effectués dans ce contexte sont soumis à la Recommandation n° R (97) 18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques. En particulier, les dispositions de la recommandation sur les statistiques exigent que les données à caractère personnel qui ont été collectées à des fins statistiques ne soient pas communiquées à des tiers pour des fins étrangères à la statistique. Par contre, ces données peuvent être communiquées sous certaines conditions à des tiers pour être traitées à d'autres fins statistiques, car il y a dans ce cas une compatibilité de finalités.

Pour la recherche de nouveaux marchés d'assurance, la gestion interne d'une compagnie d'assurance, l'activité d'actuariat et, dans la mesure du possible, les données devraient être traitées de manière anonyme ou du moins sans données d'identification directe, conformément aux principes de la Recommandation n° R (97) 18.

48. La recommandation fait allusion au principe général de la compatibilité de finalité :

– La finalité du traitement doit être déterminée lors de la collecte. Le fait de déterminer les finalités correspond, en effet, à trois objectifs: limiter l'ingérence dans la vie privée, assurer la transparence à l'égard de la personne concernée et assurer un contrôle de la finalité de traitement. Les finalités limitativement énumérées au Principe 4.4 ne

constituent pas une seule finalité générale, mais des finalités spécifiques légitimes qui découlent de l'activité d'assurance.

– Une finalité est susceptible d'évoluer avec le temps. Ainsi, les finalités auxquelles il est fait référence au Principe 4.1 sont celles énumérées au principe 4.4 sur « la finalité », mais aussi aux Principes 4.8, 8.1 et 13.1, sur le marketing direct, la communication et l'archivage ou la conservation. Dès lors, si, au moment de la collecte, toutes les finalités d'assurance énumérées au principe 4.4 n'ont pas été spécifiées, conformément à l'article 5 de la Convention 108, les données ainsi collectées peuvent être traitées ultérieurement pour une autre finalité énoncée au Principe 4.4 dans la mesure où elle est compatible avec la ou les finalité(s) antérieure(s). A titre d'exemple, les données recueillies à des fins d'établissement d'une assurance automobile pourront être utilisées à des fins d'établissement d'un dossier pour ester en justice en cas de litige entre l'assureur et la personne concernée liée par le contrat. D'un autre côté, si des données sont collectées pour une assurance santé et que, par conséquent, des données médicales sont collectées portant sur des demandes, une image claire de l'état de santé d'une personne pourrait en résulter. Certains pays ont explicitement prévu que l'utilisation de ces données pour un type d'assurance différent, tel que l'assurance-vie, constitue une forme d'utilisation incompatible. Elles ne devraient pas être utilisées pour les besoins d'une autre branche d'assurance, telle que l'assurance-vie.

– Dans certains cas, la question de la compatibilité se pose lorsque des données collectées pour un type d'assurance sont appariées avec d'autres données pour la finalité de nouveaux services financiers. En principe, un tel traitement ultérieur pourrait être considéré comme étant compatible avec la finalité d'origine. Ce traitement ultérieur peut aussi être considéré comme étant compatible lorsque des données sont collectées par une compagnie d'un groupement (une holding ou un consortium) et utilisées ensemble avec des données d'une autre compagnie du même groupement, dans des cas exceptionnels dans lesquels le groupement lui-même est le responsable du traitement.

Enfants à naître

49. **Le Principe 4.5** vise de façon spécifique, à l'instar de la Recommandation n° R (97) 5 relative à la protection des données médicales, le traitement à des fins d'assurance de données à caractère personnel relatives à l'enfant à naître. Cependant, ce principe soulève des questions de nature éthique, qui vont au-delà du champ d'application de la recommandation. Il s'agit surtout de protéger le secret des informations sur la vie privée des enfants à naître, après leur naissance. En effet, il est possible dans la plupart des pays d'assurer l'enfant à naître. Si des problèmes surviennent et que des données sont collectées, ces données datant de la grossesse pourraient être utilisées ultérieurement. Il ne s'agit pas d'établir l'autorité parentale, mais plutôt de veiller à ce que les données d'un enfant ne soient pas déjà « publiques » au moment de sa naissance. La recommandation incite à ce que des mesures soient prises pour assurer la protection des données collectées et traitées avant la naissance d'un enfant.

50. C'est pourquoi l'enfant à naître devrait bénéficier d'une protection similaire à la protection des données d'un enfant après sa naissance. A titre d'exemple, cet objectif peut être atteint en considérant des données de l'enfant à naître comme des données à caractère personnel de la mère. Suivant la tendance du droit de la famille dans les Etats membres, sauf si le droit

interne en dispose autrement, les détenteurs légaux de l'autorité parentale du futur enfant devraient pouvoir agir au nom de l'enfant à naître en tant que personne concernée. Il est entendu que, lors de l'exercice des droits d'accès et de rectification relatifs aux données de l'enfant à naître, les intérêts de la personne concernée sont dûment pris en compte.

Données sensibles

51. **Le Principe 4.6** porte sur la collecte et le traitement de données sensibles dont la définition figure au chapitre 1. Ce principe découle de l'article 6 de la Convention 108, qui prévoit que de telles données ne peuvent être traitées que moyennant des garanties appropriées prévues par le droit interne. Sous l'angle de la finalité, les données sensibles sont régies par les Principes 4.3, 4.4, 4.8, 8.1 et 13.1.

52. Le Principe 4.6 pose le principe de l'interdiction de la collecte et du traitement des données sensibles. Des exceptions à ce principe sont toutefois énumérées pour les seules fins énoncées au Principe 4.4. Ces exceptions sont les suivantes:

a. la loi prévoit telle collecte ou tel traitement ou une autorité de contrôle - au sens du Principe 15.1 - les autorise, pour autant qu'un intérêt public important le justifie. Dans ce cas, des garanties appropriées doivent être prévues par le droit interne;

b. la collecte et le traitement sont nécessaires au respect des obligations légales ou contractuelles spécifiques du responsable du traitement. Dans ce cas encore, le droit interne doit prévoir des garanties appropriées. Cette exception peut toutefois ne pas être prévue par le droit interne de certains Etats, en particulier les Etats membres de l'Union européenne, étant donné que l'article 8 de la Directive 95/46/CE ne prévoit pas une telle exception;

c. la collecte et le traitement sont nécessaires à la constatation, l'exercice ou la défense d'un droit en justice;

d. la collecte et le traitement sont nécessaires à la défense des intérêts vitaux de la personne concernée elle-même ou d'une autre personne et dans le cas où la personne concernée n'est pas en mesure de donner son consentement ;

e. la loi ne l'interdit pas et la personne concernée a donné son consentement explicite au traitement des données.

53. En ce qui concerne les données médicales, il convient de se reporter notamment à la Recommandation n° R (97) 5 relative à la protection des données médicales. Lors de l'élaboration de cette dernière, une définition assez large des données médicales avait été adoptée, précisément en vue de couvrir tous les secteurs où de telles données pouvaient être utilisées, y compris le secteur de l'assurance (voir les paragraphes 40 et 103 de l'exposé des motifs de la Recommandation n° R (97) 5). Les données relatives au tabagisme, à l'abus d'alcool ou à la consommation de drogue sont aussi considérées comme des données médicales (paragraphe 45 du rapport explicatif de la Convention 108 et paragraphe 38 de l'exposé des motifs de la Recommandation n° R (97) 5).

54. En ce qui concerne les données génétiques, il convient également de se reporter à la Recommandation n° R (97) 5 qui est conforme aux dispositions de la Convention sur les droits de l'homme et la biomédecine (STE n° 164) ouverte à la signature à Oviedo le 4 avril 1997. Cependant, la pratique des Etats membres et le régime juridique en matière de collecte et de traitement des données génétiques à des fins d'assurance ne sont pas partout uniformes, ainsi la recommandation ne préjuge-t-elle pas des développements attendus dans ce domaine, ayant trait, notamment, à la bioéthique. En effet :

a. Le principe 7 de la Recommandation n° R (92) 3 sur les tests et le dépistage génétiques à des fins médicales dispose que « les assureurs n'ont pas le droit d'exiger des tests génétiques ou d'enquêter sur les résultats de tests déjà réalisés, en tant que condition préalable à la conclusion ou à la modification d'un contrat d'assurance ».

b. A ce jour toutefois, la position des différents pays européens n'est pas uniforme en matière de collecte et de traitement de données génétiques à des fins d'assurance. Dans certains pays, par exemple, lorsque le montant d'un contrat d'assurance est élevé, il est estimé que l'assureur devrait pouvoir demander la communication des résultats de tests génétiques prédictifs. Ailleurs, l'utilisation des données génétiques à des fins d'assurance est purement et simplement interdite par la loi. Enfin, dans d'autres pays un moratoire a été proclamé.

c. Le Principe 4.9 de la Recommandation n° R (97) 5 dispose que « à des fins autres que celles prévues aux Principes 4.7 (à des fins de prévention, de diagnostic, ou à des fins thérapeutiques) et 4.8 (les besoins d'une procédure judiciaire ou d'une enquête pénale), la collecte et le traitement des données génétiques devraient en principe être permis uniquement pour des raisons de santé et notamment pour éviter tout préjudice sérieux à la santé de la personne concernée ou de tiers ».

d. L'article 12 de la Convention n° 164 dispose que les tests génétiques prédictifs ne peuvent être réalisés qu'à des fins médicales ou de recherche médicale, mais il ne dit pas si l'utilisation de ces tests est autorisée à d'autres fins, y compris des fins d'assurance. Une telle utilisation n'est-elle pas susceptible d'entraîner une discrimination des personnes sur le fondement de leurs gênes (article 11) ou d'entraver l'accès équitable de ces personnes à des soins médicaux (article 3), ce qui porterait atteinte au principe de la dignité humaine ? Une telle utilisation des données génétiques pourrait éventuellement faire l'objet des restrictions prévues à l'article 26 de cette même Convention sur la base, par exemple, de la protection des droits et libertés d'autrui. Toutefois, l'article 5 de la Convention 108 n'exclut pas que des données génétiques collectées à des fins médicales ou de recherche médicale puissent être utilisées à d'autres fins compatibles. Ces questions à mi-chemin entre la « bioéthique » et « l'infoéthique » sont l'objet de travaux spécifiques par les comités du Conseil de l'Europe en charge de l'élaboration d'un protocole additionnel sur la génétique à la Convention sur les droits de l'homme et la biomédecine. Les restrictions à la collecte et au traitement des données génétiques imposées par ce protocole additionnel s'appliqueront également aux données à caractère personnel collectées et traitées à des fins d'assurance. C'est notamment pour cette raison qu'aucune disposition sur les données génétiques n'a pas été incluse dans cette recommandation.

Données pénales

55. **Le Principe 4.7** vise à renforcer la protection d'une catégorie particulière de données à caractère personnel, à savoir les données relatives aux poursuites et aux condamnations pénales. Il s'agit de catégories de données qui sont également collectées et traitées dans le domaine des assurances. Le traitement de ces données ne peut cependant intervenir que si ces données sont nécessaires à l'existence même de l'assurance et à l'activité d'assurance. Par exemple, pour certains types d'assurance, l'assureur a besoin de vérifier si la personne concernée a fait l'objet de condamnations pénales.

56. La recommandation autorise la collecte et le traitement de ces données à des fins d'assurance si:

a. le traitement de telles données est conforme aux garanties appropriées prévues par le droit interne;

b. cela est nécessaire pour atteindre l'objectif légitime de la collecte des données. Il s'agit ici d'une application particulière du principe de proportionnalité énoncé au principe 4.1. Cette application exige toutefois que l'objectif spécifique de la collecte des données soit déterminé avec la plus grande précision;

c. la finalité de cette collecte ou de ce traitement concerne un nombre limité de finalités, à savoir:

- la préparation et la fourniture d'une police d'assurance (4.4.*a*);
- le règlement de demandes d'indemnisation ou d'autres prestations (4.4.*c*);
- la lutte à l'égard des fraudes à l'assurance (principe 4.4.*f*);

Marketing direct

57. **Le Principe 4.8** énonce des règles spécifiques en ce qui concerne la collecte et le traitement de données à caractère personnel à des fins de marketing direct pour le secteur de l'assurance. Il s'agit de permettre la prospection auprès de personnes dont les données ont déjà été collectées ou traitées à des fins d'assurance par le responsable du traitement.

a. D'après la recommandation, les données à caractère personnel devraient être collectées et traitées à des fins de marketing direct pour autant que la personne concernée ne s'y soit pas opposée, mais seulement après qu'elle en a été pleinement informée conformément au chapitre 5 :

- La collecte et le traitement de données à des fins de marketing direct pour la gamme de services à la disposition du responsable du traitement sont soumis au système du droit d'opposition. Dans ce système, le responsable du traitement peut collecter et traiter des données à des fins de marketing direct sans obligation d'exiger le consentement de la personne concernée et à condition que la personne concernée ait la possibilité de s'y opposer.

– De plus en plus de groupes ou de compagnies fournissent, entre autres services, des services d'assurance. Ainsi, il n'est pas toujours aisé de définir les limites propres d'un groupe ou d'une société au-delà desquelles il y a communication d'informations à des tiers. C'est pourquoi la communication de ces données est régie spécifiquement par le principe 8.1.*c* de la recommandation, qui prévoit également le système du droit d'opposition. Cette solution s'inspire de la Recommandation n° R (85) 20 relative à la protection des données à caractère personnel utilisées à des fins de marketing direct, qui distingue la collecte des données à des fins de marketing direct de la mise à disposition de listes à des tiers.

– Conformément au chapitre 5, il n'est pas nécessaire que le responsable du traitement informe lui-même la personne concernée de la possibilité qu'a celle-ci de s'opposer au traitement de ses données à des fins de marketing direct, mais il peut aussi donner cette information par le biais d'une information générale du public.

b. La recommandation n'entend pas exclure l'utilisation de données sensibles à des fins de marketing direct et interdire les « profils » élaborés par les compagnies d'assurance. Toutefois, l'utilisation de données sensibles requiert le consentement explicite de la personne concernée (à l'instar de l'article 8.2.*a* de la directive) pour autant que le droit interne ne s'y oppose pas, conformément au chapitre 6 sur le consentement. Ce consentement vise également celui délivré par téléphone, lors d'enquêtes téléphoniques.

5. L'information des personnes concernées

58. **Le Chapitre 5** est consacré à l'information qui doit être fournie par le responsable du traitement aux personnes concernées afin de respecter les exigences d'une collecte loyale, telles qu'elles sont énoncées à l'article 5 de la Convention 108. La recommandation établit une distinction entre ce type d'information et d'autres catégories d'informations considérées dans la Convention:

a. La Convention 108 exige en effet dans son article 8 que chaque individu puisse obtenir des informations sur tout enregistrement et sur toute communication des données à caractère personnel le concernant, et qu'il puisse ainsi éventuellement demander des modifications de ces données, voire jouir d'un droit de recours. Il s'agit là de garanties complémentaires qui ont été conçues pour permettre à toute personne de défendre ses droits vis-à-vis des fichiers informatisés, compte tenu notamment des risques que des décisions individuelles soient prises à son égard sur la base des données qui sont contenues dans ces fichiers ou qui sont communiquées à des tiers par un responsable du traitement.

b. Conformément à l'article 5 de la Convention 108, les personnes dont les données sont collectées doivent aussitôt, en principe, recevoir une information adéquate, notamment sur la nature, les caractéristiques, les circonstances et les objectifs de la collecte et du traitement. Cette information constitue non seulement un élément essentiel de la loyauté de la collecte et du traitement, mais également un moyen d'obtenir des réponses sincères et, donc, d'assurer la fiabilité des données. Ainsi, la loyauté de la collecte et la qualité des données recueillies à des fins d'assurance se rejoignent.

59. **Le Principe 5.1** énonce, aux alinéas *a* et *b*, les éléments d'information qui doivent toujours être fournis aux personnes concernées. Dans tous les cas, les personnes concernées

doivent être informées de la ou des finalité(s) pour lesquelles leurs données sont ou seront traitées et l'identité du responsable du traitement. Mais l'obligation d'information du responsable du traitement ne doit pas constituer une charge disproportionnée par rapports aux objectifs de la collecte. C'est pourquoi la recommandation énonce, à l'alinéa *c*, la liste minimale des autres informations qui doivent être, le cas échéant, fournies aux personnes concernées pour assurer le caractère loyal de la collecte au sens du principe 5.4. En particulier, toute personne concernée doit, le cas échéant, savoir quelles catégories de données sont ou seront collectées; les catégories de personnes ou d'organismes extérieurs auxquels elles peuvent être communiquées et les objectifs de cette communication; la possibilité, le cas échéant, pour la personne concernée de s'opposer, par exemple au traitement de ses données à des fins de marketing direct, de refuser son consentement et de le retirer, et les conséquences d'un tel retrait; les conditions d'exercice des droits d'accès et de rectification; et les catégories de toute autre source qui peut être consultée.

60. **Le Principe 5.2** est relatif à l'information des personnes concernées lorsque la collecte des données est effectuée auprès de celles-ci. Il précise que l'information doit être communiquée au plus tard au moment de la collecte, sauf si les personnes concernées ont déjà obtenu les informations par d'autres voies. Cette exception au devoir d'information, lorsque la personne concernée a déjà été informée, devrait être interprétée de manière restrictive. Par exemple, lors d'un démarchage téléphonique, il ne devrait pas être suffisant qu'en début de conversation on informe la personne d'une collecte et d'un traitement possible pour que cette information soit valable dans le cadre de toutes les relations contractuelles éventuelles futures. Cependant, la possibilité de ne pas transmettre ces informations peut être admise, si cette information a été fournie par écrit, peu de temps auparavant, dans le cadre des négociations portant sur le même contrat.

61. **Le principe 5.3** envisage les cas où la collecte des données est effectuée auprès d'un tiers. Il prévoit que l'information doit être fournie à la personne concernée par n'importe quel moyen, soit lors de l'enregistrement des données, soit, si une communication à un tiers est envisagée, lors de la première communication des données au plus tard.

62. Cette forme de collecte ne peut, à l'évidence, pas se dérouler dans les mêmes conditions d'information que celles d'une collecte auprès des personnes concernées. L'obligation d'informer les personnes concernées doit être adaptée aux circonstances particulières des collectes à des fins d'assurance auprès de tiers. En particulier, outre qu'il est inutile, comme dans le cas de la collecte auprès des personnes concernées, d'informer celles-ci une seconde fois lorsqu'il est établi qu'elles ont déjà reçu l'information décrite au Principe 5.1, des dérogations à l'information sont prévues lorsqu'en pratique cette information s'avère manifestement déraisonnable ou infaisable, ou encore lorsque le traitement ou la communication des données à des fins d'assurance sont expressément prévus par le droit interne. Dans ces deux derniers cas, des garanties appropriées doivent cependant être prévues par le droit interne et mises en oeuvre par le responsable de traitement. Celles-ci peuvent prendre la forme, par exemple, de mesures de publicité générale.

63. D'après **le Principe 5.4,** une information trop détaillée peut constituer une charge disproportionnée et inutile aussi bien pour les professionnels de l'assurance que pour la personne concernée. Dès lors, l'information fournie par le responsable du traitement devrait être proportionnée par rapport aussi bien aux intérêts des personnes concernées qu'aux circonstances,

aux enjeux et à la portée de la collecte. En particulier, la terminologie utilisée et les degrés de détail ou de généralité de l'information devraient être de nature à permettre à la personne interrogée de comprendre dans les grandes lignes les objectifs et l'importance de la collecte de données. Le caractère loyal de la collecte s'apprécie tout particulièrement à la lumière de l'information transmise par le responsable de traitement. Enfin, l'étendue de l'information devrait permettre à la personne interrogée de manifester un consentement éclairé lorsque le consentement est la base de licéité du traitement.

64. **Le Principe 5.5** porte sur l'information lorsque des données relatives à des personnes légalement incapables sont collectées à des fins d'assurance. Il s'agit ici de personnes qui, selon le droit interne, ne sont pas en mesure d'agir en leur propre nom. Cette catégorie de personnes recouvre aussi bien les mineurs que les personnes privées de discernement et qui, dès lors, ne sont pas à même de formuler un refus ou un consentement libre et informé.

a. Lorsque des personnes légalement incapables sont concernées par une collecte des données à caractère personnel, les informations y relatives doivent être fournies à leurs représentants légaux. Toutefois, dans certains Etats membres, le droit interne permet à certaines catégories de personnes légalement incapables d'agir en leur propre nom ; dans ces cas particuliers, l'information peut être adressée directement aux personnes concernées.

b. Par ailleurs, le Principe 5.5 requiert l'information directe des personnes légalement incapables qui sont néanmoins en mesure de comprendre. Dans certains domaines particulièrement sensibles, tel le cas de l'assurance-vie, cette information est importante pour s'assurer du fait que le consentement est vraiment libre.

65. Le **Principe 5.6** est inspiré directement de l'article 9 de la Convention 108, qui définit les limites autorisées pour toute ingérence perpétrée à l'égard des droits reconnus par la Convention 108. La Convention prévoit qu'il est possible de déroger à l'information des personnes lorsqu'une telle dérogation est prévue par la loi, et qu'elle constitue une mesure nécessaire dans une société démocratique à la défense d'un certain nombre de buts légitimes limitativement énumérés. Cette formulation est inspirée du deuxième paragraphe de l'article 8 de la Convention européenne des Droits de l'Homme, mais, parmi ces buts, la recommandation ne fait pas figurer la sécurité de l'Etat, la sûreté publique ou les intérêts monétaires de l'Etat. A titre d'exemple, il peut être possible de limiter l'octroi de l'information si cela est nécessaire à la protection de la personne concernée ou à la protection des droits et libertés d'autrui. La limitation de l'information des bénéficiaires d'un contrat sur la vie, par exemple, peut-être motivée par le droit au respect de la vie privée des assurés.

6. Le consentement

66. **Le Chapitre 6** est consacré au consentement des personnes concernées lorsqu'elles ont la faculté d'accepter ou de refuser que leurs données soient collectées et traitées à des fins d'assurance. Ce chapitre se fonde sur l'article 5 de la Convention 108 et sur le Principe 4.3 de la recommandation, au sens desquels le consentement constitue l'une des conditions essentielles de la loyauté et de la licéité des collectes. Il convient, à cet égard, de rappeler que le consentement spécifique à la protection des données doit être distingué des conditions de validité du consentement dans le cadre d'un contrat. En outre, le principe 4.3 de la recommandation considère nettement le contrat et le consentement comme des bases de licéité distinctes.

67. **Le Principe 6.1** définit les caractéristiques et les modalités générales d'exercice du consentement. Le consentement de la personne concernée doit être « libre, spécifique et informé ». Il doit en outre être donné de façon indubitable.

a. Le consentement comporte donc quatre conditions cumulatives:

– « libre », il ne doit pas avoir été obtenu, notamment, sous la contrainte ou sous l'effet d'une influence ou d'une pression abusives ;

– « spécifique », il doit porter sur une ou plusieurs opérations relatives au traitement des données et ne doit pas être entendu comme une licence générale accordée par la personne concernée au responsable du traitement, à moins que la personne concernée ait souhaité de manière indubitable octroyer ce type de licence générale, pour une ou plusieurs opérations;

– « informé », il signifie que la personne concernée a été préalablement informée des finalités et des modalités de la collecte et du traitement auxquels elle consent, conformément au chapitre 5 de la recommandation ;

– « indubitable », il ne suffit pas de considérer que la personne concernée est présumée avoir donné son consentement.

b. La forme dans laquelle le consentement est donné doit être renforcée lorsqu'il s'agit de collecter et de traiter des données sensibles telles que définies au Chapitre 1 ; le consentement doit alors être donné par la personne concernée non pas de manière indubitable comme décrit au point précédent, mais de manière explicite, supposant une manifestation expresse de la volonté. Il peut y avoir des cas où le droit interne prévoit que l'interdiction de collecter ou traiter des données sensibles ne peut être levée que par le consentement de la personne concernée. Tel est le cas dans certains pays en ce qui concerne, par exemple, le traitement des données médicales ou génétiques.

68. **Le Principe 6.2** porte sur le consentement lorsque des données relatives à des personnes légalement incapables sont collectées et traitées à des fins d'assurance. En principe, ce consentement, tel qu'il est caractérisé dans le Principe 6.1, doit être manifesté par le responsable légal de la personne concernée (les parents, le tuteur ou toute autre personne, autorité ou instance qui, au sens de la loi, assume la responsabilité légale de la personne concernée). Toutefois, lorsque le droit interne prévoit que certaines catégories de personnes légalement incapables peuvent agir en leur propre nom, celles-ci peuvent manifester leur consentement ou leur opposition. Conformément au Principe 5.5, qui encourage l'information des personnes légalement incapables qui sont en mesure de comprendre, les rédacteurs ont estimé que, sauf opposition du droit interne, ces personnes devraient avoir la possibilité d'exprimer leur souhait de conclure ou non l'assurance. Il ne s'agit pas ici d'un consentement au sens strict (celui-ci relève en dernière instance du responsable légal), mais d'une mesure visant à associer ces personnes au processus de réflexion et de décision quant au consentement.

69. Le **Principe 6.3** précise que lorsque cela est possible, on puisse prendre en considération le souhait d'une personne considérée juridiquement comme incapable et, par exemple, lorsqu'elle a été informée d'une collecte ou d'un traitement de données la concernant et qu'elle était en mesure de comprendre, à moins que le droit interne s'y oppose.

7. Collecte et traitement par un sous-traitant

70. Le **Chapitre 7** énonce des règles spécifiques en ce qui concerne les conditions dans lesquelles le responsable du traitement peut sous-traiter la collecte et le traitement de données à caractère personnel à des fins d'assurance. Pour que la sous-traitance soit possible, elle ne doit évidemment pas contredire les obligations légales et contractuelles en matière de sécurité ou de confidentialité.

71. Le **Principe 7.1** évoque la possibilité offerte au responsable du traitement, tel que défini au Chapitre 1, de déléguer la collecte et le traitement de données à caractère personnel à des fins d'assurance déterminées à un sous-traitant qui peut être généralement toute personne physique ou morale, toute autorité publique, tout service ou tout organisme, dès lors que ce sous-traitant s'engage à n'agir que sous la seule instruction du responsable du traitement et à respecter les dispositions du Chapitre 11 relatif à la sécurité.

72. Le **Principe 7.2** énonce les obligations incombant au responsable du traitement en ce qui concerne le choix du sous-traitant. Ainsi, il doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures techniques et organisationnelles des traitements à effectuer. Ces mesures sont prévues au Chapitre 11 de la recommandation sur la sécurité des données. Enfin, il a l'obligation de s'assurer que les collectes et les traitements effectués sont conformes à ses instructions.

73. Une conséquence logique de ce qui vient d'être dit est le fait que la recommandation exige dans le **Principe 7.3** que la sous-traitance soit l'objet d'un contrat ou de tout autre acte juridique nécessaire à la matérialisation des obligations susmentionnées. Il est clair aussi que le responsable du traitement reste tenu de remplir l'ensemble des obligations prévues par la présente recommandation en ce qui concerne les traitements qui font l'objet de traitements en sous-traitance.

8. Communication à d'autres fins

74. Ce chapitre établit les conditions permettant que des données à caractère personnel collectées et traitées pour les finalités prévues dans la recommandation puissent être communiquées à un tiers en vue d'un nouveau traitement à d'autres fins que des fins d'assurance.

a. En premier lieu, la communication constitue un traitement conformément à la définition retenue au chapitre 1. Par conséquent, toute communication de données à caractère personnel doit se faire en conformité avec l'ensemble des principes de la recommandation.

b. Au-delà des finalités énoncées au Principe 4.4, la communication est autorisée :

– lorsqu'elle est prévue par la loi, pour un motif d'intérêt public important, tel que la répression des infractions pénales. Conformément à l'article 9 de la Convention 108, cette communication, dans la mesure où elle constitue une ingérence au droit au respect de la vie privée, ne doit intervenir que si elle est prévue par la loi et constitue une mesure nécessaire dans une société démocratique, aux fins prévues par cet article ;

– si la personne concernée donne son consentement, dans les conditions du chapitre 6, sans que le droit interne ne s'y oppose ;

– à des fins de prospection dans les conditions prévues par le principe 8.*c* ; toutefois, la Recommandation n° R (85) 20 relative à la protection des données à caractère personnel utilisées à des fins de marketing direct prévoit qu'en cas de mise à disposition de listes à des tiers, « à moins que la personne concernée n'ait donné son consentement, les listes ne devraient pas fournir d'informations pouvant porter atteinte à sa vie privée ». Tel pourrait être le cas, par exemple, des « profils » révélant des traits de la personnalité des personnes concernées.

– dans l'intérêt légitime du responsable du traitement, à l'instar du Principe 4.3.*d* et dans les mêmes conditions que ce principe.

9. Décisions individuelles automatisées

75. Les décisions individuelles automatisées sont celles qui sont prises sur le seul fondement d'un traitement automatisé destiné à évaluer les aspects de la personnalité des personnes concernées, sur la base de critères préétablis ou de résultats statistiques. Dans le secteur des assurances, le recours à des décisions individuelles automatisées est chose courante et constitue parfois une nécessité pour le bénéfice des personnes concernées et des clients.

76. Le **Principe 9.1** pose le principe de l'interdiction de certaines décisions individuelles automatisées lorsqu'elles produisent des effets juridiques à l'égard des personnes concernées ou qu'elles les affectent de manière significative. Parmi ces décisions, il convient de mentionner notamment les décisions relatives à l'octroi ou à l'étendue de l'assurance ou au versement d'autres prestations. En revanche, le simple fait d'adresser des prospectus publicitaires à une liste de personnes déterminées par ordinateur ne constituerait pas une décision susceptible d'être interdite en application du Principe 9. Il doit s'agir également d'une décision prise sur le seul fondement d'un traitement automatisé : ce qui est prohibé, c'est la stricte application par l'utilisateur des résultats produits par le logiciel ou le système-expert, sans place donnée à l'appréciation humaine. L'informatique peut évidemment être utilisée pour fournir une aide à la décision, notamment dans l'appréciation du risque pour lequel une assurance est demandée.

77. La recommandation prévoit donc la possibilité de recourir à de telles décisions si elles satisfont à une demande exprimée par la personne concernée en vue de la conclusion ou de l'exécution d'un contrat d'assurance ou si la personne concernée est admise à faire valoir son point de vue afin de garantir la sauvegarde de ses intérêts légitimes. De telles décisions peuvent également intervenir si elles sont prévues par la loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

10. Droits d'accès et de rectification

78. Le **Chapitre 10** correspond aux droits prévus à l'article 8 de la Convention 108: toute personne doit savoir si des données la concernant ont été obtenues et sont détenues par le responsable du traitement. Elle doit pouvoir avoir accès aux données à caractère personnel la concernant et doit également pouvoir obtenir du responsable du traitement que ces données soient rectifiées lorsqu'elles sont fausses ou périmées. Ce chapitre vise notamment à permettre aux personnes de se prémunir contre le risque que des décisions ou des mesures individuelles soient prises à leur égard sur la base de données fausses ou périmées qui seraient contenues dans des fichiers et qui auraient été ou pourraient être communiquées à des tiers par le responsable du traitement. L'exercice du droit d'accès doit être libre ; la personne concernée ne doit pas, par exemple, être obligée par un tiers d'exercer son droit d'accès en vue de lui communiquer les données ou de les communiquer à une autre personne. Par ailleurs, les auteurs de la recommandation ont souligné que le droit d'accès de la personne concernée doit pouvoir être mis en oeuvre sans porter atteinte au secret des affaires ni à la propriété intellectuelle, par exemple au droit d'auteur protégeant le logiciel, notamment, en cas d'accès à la connaissance de la logique qui sous-tend le traitement automatisé. Il va sans dire que les personnes concernées devraient exercer leur droit d'accès de manière raisonnable et éviter d'effectuer des demandes trop fréquentes et abusives.

79. Le **Principe 10.1** énumère les informations auxquelles la personne concernée doit pouvoir accéder si elle en fait la demande. Il s'agit :

a. de la confirmation que des données la concernant sont ou ne sont pas collectées ou traitées; et,

b. sous une forme intelligible, des données la concernant et des informations portant au moins :

- sur les finalités de l'opération de traitement,
- sur les catégories de données sur lesquelles porte le traitement ;
- sur les destinataires ou les catégories de destinataires auxquels les données sont communiquées, et
- sur l'origine des données. L'information sur la source des données ne doit être fournie que si elle est disponible.

c. de la connaissance de la logique qui sous-tend le traitement automatisé des données la concernant, au moins dans le cas de décisions individuelles automatisées.

80. Le **Principe 10.2** réitère une dérogation prévue par l'article 9 de la Convention 108, qui prévoit que l'accès d'une personne à ses données peut être limité pour les besoins de la répression des infractions pénales et pour ne pas nuire aux résultats d'une enquête en cours. La collecte de données ayant pour finalité la détection et la répression des fraudes est prévue par le Chapitre 4. A l'issue de l'enquête, le responsable du traitement est tenu d'informer la personne concernée qu'elle peut accéder aux données qui la concernent. Les rédacteurs ont toutefois songé à des cas où la limitation à l'accès doit perdurer sans pouvoir dire à quel moment et si elle devra cesser.

81. Le **Principe 10.3** porte sur le droit dont disposent les personnes concernées d'exiger l'effacement, le verrouillage ou la rectification de leurs données à des fins d'assurance si elles sont inexactes ou si elles ne sont pas nécessaires. Dans certains cas, la rectification à elle seule n'est pas suffisante et la réparation du préjudice subi par la personne concernée ou le rétablissement d'un traitement loyal peut exiger l'effacement, voire la destruction ou le verrouillage, des données. Le Principe 10.5 énonce que si le responsable du traitement a communiqué ces données, il doit également informer les personnes auxquelles il les a communiquées des rectifications, effacements, destructions ou verrouillages auxquels il a procédé, à moins que cela ne s'avère manifestement déraisonnable ou infaisable.

82. Le **Principe 10.4** dispose que toute limitation ou tout refus d'accorder l'accès, la rectification, l'effacement ou la destruction des données doit être signifié à la personne concernée par écrit et en motivant la décision, à moins que l'explication des motifs ne porte préjudice à la raison même du refus d'accorder l'accès. Tel est le cas notamment pour les refus ou délais au droit d'accès en vertu du Principe 10.2. Dans ce cas, il convient d'informer la personne concernée de son droit de saisir l'autorité de contrôle compétente. En outre, en vertu de l'article 5.*d* de la Convention 108, le responsable du traitement est invité à mettre à jour les données, si cela est nécessaire.

83. Le **Principe 10.5** dispose que le responsable du traitement a l'obligation d'informer les tiers auxquels il a communiqué les données d'une personne, que les données de celle-ci ont été rectifiées, effacées ou verrouillées, à moins que cela soit manifestement déraisonnable ou infaisable.

84. D'après le **Principe 10.6,** le responsable du traitement doit permettre que la personne concernée exerce son droit d'accès « sans délais ou frais excessifs ». Il peut aussi prévoir une gratuité complète en ce qui concerne l'exercice de ce droit. La personne qui exerce le droit d'accès peut être la personne concernée ou son représentant légal. Cette personne est habilitée à solliciter toute information nécessaire sur le traitement et sur les données la concernant.

11. Sécurité des données

85. Le **Principe 11.1** porte sur les mesures techniques et d'organisation qui doivent être prises pour assurer la sécurité des données. La sécurité des données garantit notamment la confidentialité, l'intégrité et la disponibilité des données. A cet égard, pour assurer la protection des données à caractère personnel, des précautions matérielles doivent être prises par le responsable du traitement afin de prévenir les accès ou les utilisations illicites des données, autant par accident que par malveillance. En outre, des mesures techniques et organisationnelles doivent faire l'objet d'un examen périodique. Elles doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et la nature des données à protéger.

86. Les mesures de sécurité exigées par le **Principe 11.2** couvrent notamment les attributions et les habilitations des services et des personnes en charge de la sécurité. Elles comprennent aussi les mesures concernant l'accès aux installations et aux documents (*a*, *b*, *c* et *e*), ainsi que le déplacement des supports de données (*d*, *f*, *h*). Elles comprennent enfin les procédures, clefs logiques, programmes de traitement ainsi que le cryptage ou le brouillage des données (*g* et *i*). La recommandation détaille la liste de mesures de sécurité nécessaires pour garantir notamment la

confidentialité, l'intégrité et la disponibilité des données. Il s'agit d'une liste minimale correspondant aux normes nationales et internationales de sécurité du point de vue de la protection des données.

87. Le **Principe 11.3** est une conséquence logique du principe précédent. Il oblige le responsable du traitement à établir un règlement interne portant sur les mesures techniques et organisationnelles mises en oeuvre pour respecter les exigences de protection des données de cette recommandation. A cet égard, les mesures de sécurité incombent autant au responsable du traitement et à ses sous-traitants qu'au bénéficiaire d'une communication de données à caractère personnel à des fins d'assurance. Il incombe au responsable du traitement d'informer de leurs devoirs les personnes qu'il fait intervenir dans la collecte et le traitement des données. Ces personnes s'engagent formellement à respecter les mesures de sécurité.

88. Le **Principe 11.4** évoque la faculté qu'ont les entreprises de désigner une personne qui serait chargée du contrôle de la mise en oeuvre des principes de la protection des données dans l'entreprise. Cette personne, qui ne devrait pas exercer des fonctions incompatibles avec cette mission de supervision, conseillerait l'entreprise sur toutes les questions liées à la protection des données et, notamment, sur les mesures techniques et organisationnelles à mettre en oeuvre, et serait son interlocuteur à l'égard des autorités nationales chargées du contrôle de la protection des données.

12. Flux transfrontières de données

89. Le **Principe 12.1** porte sur les flux internationaux de données à caractère personnel à des fins d'assurance. La nécessité de garantir l'équilibre entre la libre circulation de l'information et le respect du droit à la vie privée s'applique également à l'échange transfrontière des données à caractère personnel. En effet, la mobilité croissante des personnes et la globalisation des activités économiques entraînent un besoin accru d'information. Le progrès des technologies de l'information et des télécommunications influencent de manière déterminante le secteur des assurances. Il convient donc que les assureurs garantissent la protection des données, quel que soit le support utilisé pour le transfert des données, y compris les inforoutes.

90. Le **Principe 12.2** illustre l'application des dispositions de l'article 12 de la Convention 108 dans le contexte des flux transfrontières de données d'assurance. Il concerne les pays qui sont parties à la Convention 108 et qui ont une législation qui apporte une protection des données équivalente. Il n'y a aucune raison de restreindre le libre flux transfrontière des données à des fins d'assurance entre des personnes, des entreprises ou des institutions publiques ou privées sises sur le territoire de ces Parties. Le transfert de données à des fins d'assurance à destination d'un Etat tiers via le territoire d'une Partie à la Convention 108 ne doit pas avoir pour objet de contourner les législations en vigueur sur la protection des données.

91. Le **Principe 12.3** autorise également le flux transfrontière des données à caractère personnel à des fins d'assurance, au départ d'Etats qui appliquent la présente recommandation vers des personnes, entreprises ou institutions sises sur le territoire d'Etats parties à la Convention 108 qui assurent un niveau adéquat de protection.

92. Le **Principe 12.4** porte sur l'éventualité d'un flux de données à caractère personnel à des fins d'assurance vers des Etats qui n'assurent pas une protection adéquate. A moins que le droit

interne de l'Etat d'où les données sont expédiées n'en dispose autrement, un tel flux ne doit avoir lieu, en principe, que si l'une des deux conditions suivantes a été remplie:

a. soit les personnes concernées ont été informées de la possibilité que leurs données soient communiquées vers un Etat qui n'offre pas des garanties de protection équivalentes à celles en vigueur dans leur pays et ces personnes ont donné leur consentement à un tel flux de façon non ambiguë ;

b. soit des dispositions spécifiques ont été prises, notamment dans le cadre d'un engagement contractuel, afin que les mesures de protection et de sécurité soient conformes aux principes de la Convention 108 et aux dispositions de la recommandation.

13. Conservation des données

93. Le **Principe 13.1** porte sur la conservation et la destruction des données à caractère personnel qui ont été collectées à des fins d'assurance.

a. Conformément à l'article 5.*e* de la Convention 108, ce principe exige que les données soient détruites ou effacées dès qu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées et traitées. Les données conservées par les entreprises ne doivent pas être effacées par celles-ci dans le but d'effacer les preuves susceptibles de démontrer leur responsabilité en invoquant le respect de ce principe. Ceci vise certaines situations particulières telles que, par exemple, la spoliation des biens des juifs pendant la deuxième guerre mondiale et l'indemnisation des ayants droit grâce aux archives privées de certaines entreprises.

b. Ce principe rappelle également que des données peuvent être conservées à des fins statistiques et de recherche scientifique ou à d'autres fins si une telle conservation est prévue par la loi. La recherche en matière d'histoire fait naturellement partie de la recherche scientifique. A cet égard, il est un fait que de plus en plus d'entreprises établissent leurs propres archives et que ces archives sont largement utilisées par la communauté des historiens. Dans ce cas, les données d'assurance pour les fins susmentionnées ne peuvent être conservées que moyennant des garanties appropriées, par exemple l'archivage séparé et l'accessibilité de certaines données uniquement à ces fins.

94. Le **Principe 13.2** rappelle qu'il peut y avoir un intérêt pour les assureurs de conserver des données de personnes auxquelles il a été refusé de fournir une assurance. Il s'agit notamment pour les assureurs de se prémunir contre les cas de fraude. En outre, s'il est vrai que des délais de conservation ne sont pas faciles à établir, ils sont toutefois nécessaires pour ne pas conduire à des abus et à la constitution de listes noires.

14. Recours

95. Le **Principe 14** rappelle les dispositions de l'article 10 de la Convention 108. Si des règles spécifiques émanant du secteur professionnel considéré sont utiles à la mise en oeuvre d'une protection effective, des sanctions et des recours appropriés doivent être prévus par le droit interne. Selon le système juridique propre à chaque Etat, ces sanctions ou ces recours seront

d'ordre civil, administratif ou pénal. Disposer d'un recours approprié implique cependant aussi la possibilité de recourir à une autorité nationale au sens du Principe 15.1 suivant.

15. Garanties pour le respect des principes

96. Le **Principe 15.1** établit le principe suivant lequel chaque Etat devrait établir une autorité de contrôle exerçant ses fonctions en toute indépendance, à moins qu'une telle autorité n'ait déjà été instituée et qu'elle ait compétence pour connaître des violations des dispositions du droit interne mettant en oeuvre les principes de la recommandation. En adoptant une loi en matière de protection des données, la plupart des pays se sont dotés de telles autorités de contrôle.

97. Le **Principe 15.2** énonce une garantie supplémentaire assurant le respect des principes de la protection des données. Cette obligation incombe au responsable du traitement et vise à rendre public, de manière appropriée, par exemple par des campagnes de presse, les traitements effectués et, notamment, les informations les plus pertinentes concernant ce traitement.