



LA RECOMMANDATION (2016)8 DU CONSEIL DE L'EUROPE SUR L'UTILISATION DES DONNÉES DE SANTÉ À DES FINS D'ASSURANCE

*RECOMMENDATION (2016)8 OF THE COUNCIL OF EUROPE
ON THE PROCESSING OF PERSONAL HEALTH-RELATED DATA
FOR INSURANCE PURPOSES*

Par Christian BYK*

SANTÉ ET ASSURANCES

RÉSUMÉ

La réglementation du marché des assurances est depuis longtemps l'affaire de l'Union Européenne alors que la protection des données et la biomédecine sont l'une des activités phare du Conseil de l'Europe. En adoptant ce texte visant à prendre en compte les possibles utilisations des données de santé, y inclus les données génétiques, le Conseil s'inscrit donc dans la continuité de ses travaux.

MOTS-CLÉS

Conseil de l'Europe, Assurance, Données de santé, Génétique, Droits de l'homme.

ABSTRACT

The regulation of the insurance market has long been the business of the European Union, while data protection and biomedicine are one of the Council of Europe's flagship activities. By adopting this text to take into account the possible uses of health data, including genetic data, the Council is thus continuing its work.

KEYWORDS

Council of Europe, Insurance, Health data, Genetics, Human rights.

* Magistrat, Secrétaire général, Association internationale droit, éthique et science, Ancien conseiller spécial pour la bioéthique du Secrétaire général du Conseil de l'Europe.

Si la réglementation du domaine des assurances, au sens du marché et de la protection du consommateur, est depuis longtemps l'apanage de l'Union Européenne (Jcl Européen, Droit européen des assurances, fascicule 1010), on sait que la protection des données et les questions relevant des droits de l'homme et de la biomédecine sont, elles, depuis des décennies, l'une des activités phare du Conseil de l'Europe.

Dès lors, en adoptant ce nouveau texte le Conseil ne fait qu'inscrire sa démarche dans la continuité de ses travaux, y compris de ses réflexions visant à prendre en compte les possibles utilisations de nouvelles données de santé, celles issues de tests génétiques.

Outre des dispositions générales applicables à tous les traitements de données de santé, le texte contient aussi des dispositions spécifiques aux données génétiques ainsi qu'aux risques, dispositions que nous ne traiterons pas ici. Les dispositions générales concernent en premier lieu l'objet de la Recommandation et certaines définitions ainsi que les règles applicables à l'ensemble des données de santé.

I. LES DISPOSITIONS GÉNÉRALES PROPREMENT DITES

A. Objet et champ d'application

- En affirmant que la Recommandation « a pour objet de garantir les droits fondamentaux des personnes, sans discrimination, dans le cadre des contrats d'assurance », le texte s'inscrit nettement dans une démarche aujourd'hui



partagée par le Conseil de l'Europe et l'Union Européenne, consacrer la protection des données individuelles de santé dans le cadre de la protection des droits fondamentaux. La Recommandation, qui concerne autant les Etats mais que les sociétés d'assurance (para.1.3 du rapport explicatif), laisse ainsi à ces acteurs le soin de jouer un rôle essentiel dans la concrétisation des dispositions qu'elle met en avant. A défaut, la démarche conventionnelle retrouverait toute sa légitimité.

- Quant aux contrats concernés, il s'agit des contrats, individuels ou collectifs, à souscription obligatoire ou volontaire, dont le principal risque couvert est lié à la santé, à l'intégrité physique, à l'âge ou au décès, tels que les contrats assurant des prestations de soins en cas de maladie, d'incapacité, d'accident, de retraite, de dépendance ou garantissant le versement d'un capital ou d'une rente en cas de décès ou de survie (I.2). Et cela représente une masse financière très importante !

B. Définitions

- Le terme « assuré » est défini conformément au droit classique des assurances et l'assureur se limite à l'assurance et à la réassurance.

- Le terme « examen » inclut tout test génétique ou non génétique ayant une valeur diagnostique ou prédictive. Quant à l'expression «test génétique », elle est définie conformément à l'article 2 du Protocole additionnel à la Convention sur les Droits de l'Homme et la biomédecine relatif aux tests génétiques à des fins médicales. De même, « le terme « traitement de données à caractère personnel » est défini sur la base de l'article 2, alinéa c, de la Convention STE n° 108 » (para.4.16 rapport explic.).

II. LES RÈGLES APPLICABLES À L'ENSEMBLE DES TRAITEMENTS DES DONNÉES DE SANTÉ

Ces principes tirent les conséquences de la philosophie générale du Conseil de l'Europe dans le domaine de l'assurance et de la santé. Celle-ci, qui est exprimée dans le préambule de la Recommandation, reconnaît qu'il existe une légitimité sociale et pratique à l'emploi du mécanisme de l'assurance privée dans le domaine de la santé. Cette reconnaissance est d'abord celle du constat d'une réalité factuelle (« l'essor important des contrats d'assurance privés couvrant un risque lié à la santé ») mais elle est aussi d'ordre sociologique et politique (« conscient du rôle que l'assurance privée volontaire peut jouer pour compléter (et parfois même suppléer) la couverture de ces risques par la sécurité sociale ou d'autres assurances publiques ou obligatoires »).

Toutefois, assumant son rôle d'organisation en charge de « l'harmonisation des législations sur des questions d'intérêt commun » et plus particulièrement la garantie du respect des droits fondamentaux de la personne, et rappelant les textes normatifs qu'il a déjà adoptés en ce domaine (la Convention pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine (« Convention sur les droits de l'homme et la biomédecine ») (STE n° 164), la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE no 108) ; la Recommandation Rec(2002)9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance ; la Recommandation Rec(97)5 relative à la protection des données médicales ; ainsi que la Charte sociale européenne révisée (STE no 163) et le Code européen de sécurité sociale (STE no 48)), le Conseil propose par ce nouveau texte « d'établir un juste équilibre entre les contraintes liées à la nature du contrat d'assurance privé, la protection des intérêts individuels des assurés et l'importance sociale de la couverture de certains risques ».

C'est pourquoi les principes énoncés dans le Chapitre II s'inspirent notamment du principe de loyauté et de licéité du traitement des données consacré à l'article 5 de la Convention STE n° 108.

A. « Principe 1 – Les assureurs devraient justifier le traitement de données à caractère personnel relatives à la santé »

« Tout en reconnaissant l'intérêt légitime de l'assureur à l'évaluation du niveau de risque présenté par l'assuré(e) », la Recommandation n'en exige pas moins de l'assureur qu'il démontre que le traitement des données à caractère personnel est nécessaire à l'évaluation du risque. En outre, cette nécessité doit être établie tant au regard de la finalité du traitement que des caractéristiques des données étudiées. Les conditions comme les modalités du traitement doivent, en tout état de cause, être conformes au principe de proportionnalité. Ce sont précisément des raisons liées au respect de ce principe qui justifient l'existence d'une limitation et de plusieurs interdictions en matière de traitement des données de santé à des fins d'assurance.

1. Conditions et modalités du traitement

La Recommandation fixe, pour justifier le traitement de données, quatre conditions (II principe 1.5) :

« 1° la finalité du traitement a été précisée et la pertinence des données a été dûment justifiée ».



Nulle surprise à cet égard: les données ne peuvent être traitées qu'à des fins précisées – en relation avec certaines maladies ou risques, par exemple, et pas seulement à des fins d'évaluation de tout risque en général) et ces données doivent avoir une pertinence, c'est-à-dire, être signifiante dans le cadre de cette finalité (note l'exposé des motifs définit la pertinence comme « l'information reconnue comme appropriée pour l'appreciation de l'état de santé d'un assuré et l'évaluation des risques relatifs à sa santé future » para.19).

« 2° la qualité et la validité des données sont conformes aux normes scientifiques et cliniques généralement reconnues ».

La pertinence suppose, en effet, que les données répondent à des critères de qualité conformes à l'état de la science et ce afin de réaliser une évaluation rigoureuse et fiable du risque. S'agissant de la provenance des données, l'exposé des motifs précise que « ces données peuvent comprendre des données relatives à la santé existantes, résultant d'examens antérieurs ou d'examens demandés par des assureurs » (para.20).

« 3° les données résultant d'un examen prédictif ont une valeur prédictive positive élevée ».

Il s'agit de souligner que le caractère prédictif d'un examen n'est pas en soi suffisant pour caractériser la pertinence exigée. Il convient que cette prédictivité présente un caractère élevé, étant, par ailleurs, précisé que « Cette observation ne vaut pas seulement pour les examens prédictifs, mais concerne aussi les examens entrepris à des fins diagnostiques qui produisent, entre autres, des données ayant une valeur prédictive » (para.21).

« 4° le traitement est dûment justifié dans le respect du principe de proportionnalité en relation avec la nature et l'importance du risque considéré ».

Pour apprécier le respect de ce principe, l'exposé des motifs nous donne quelques indications : « il convient de tenir dûment compte des droits concernés, en particulier le droit au respect de la vie privée et le respect de la volonté de ne pas être informé (voir l'Article 10 (2) de la Convention ETS n° 164, aussi appelé « droit de ne pas savoir »)... mais aussi d'autres droits fondamentaux comme le droit de ne pas subir de discrimination. A cet égard, la collecte et la transmission, à des fins d'assurances, de données relatives à la santé obtenues au moyen de technologies portables (par exemple des applications de santé) comporte un risque particulier de discrimination des personnes exerçant leur droit de ne pas partager des données recueillies par de tels dispositifs » (para.22).

. Quant aux modalités de collecte des données liées à la santé, le texte vise à s'assurer de la loyauté des modalités de collecte par deux mesures :

La première concerne la pratique du questionnaire pour lequel il adopte une approche similaire à celle fixée par

la jurisprudence française, à savoir que « les questions posées par l'assureur devraient être claires, intelligibles, directes, objectives et précises ».

Afin de renforcer cette compréhension, s'y ajoute une seconde mesure, à savoir que : « les assureurs devraient faciliter l'accès à une personne de contact ayant la compétence et l'expérience nécessaires pour répondre à toute difficulté de compréhension concernant les documents pour la collecte de données à caractère personnel liées à la santé ». Pour rendre cette mesure véritablement effective, il aurait peut-être été souhaitable de préciser que cette personne devrait être indépendante de l'assureur.

2. Limitation et interdictions :

le texte contient une limitation et trois interdictions

. La limitation vise le traitement des données à caractère personnel relatives à la santé de membres de la famille de l'assuré(e) à des fins d'assurance, qui ne devrait être autorisé que si cela est spécifiquement prévu par la loi. En effet, les assureurs ont pris l'habitude d'interroger les candidats à l'assurance sur leurs antécédents familiaux, ce qui permet de contourner l'interdiction que la loi fait, dans certains pays comme la France, d'utiliser les résultats de tests génétiques et a aussi l'avantage de limiter des demandes d'examens médicaux qui peuvent être coûteux. Cependant, cette pratique présente des inconvénients pour la protection des droits des personnes : pour l'assuré, sa fiabilité reste incertaine et, pour les membres de sa famille, elle peut porter une atteinte excessive au respect de leur vie privée. C'est pourquoi, la recommandation ne permet cette pratique que si elle est spécifiquement prévue par la loi, ce que l'exposé des motifs entend cependant très largement (comprend les codes, la législation, les règlements, les lignes directrices et autres dispositions légales, ainsi que des codes de bonnes pratiques et des accords, accessibles au public, conclus entre Etat membre et assureurs. Elle comprend également les décisions de justice ainsi que les aspects du droit des contrats et de common law ayant trait aux principes régissant les contrats d'assurance). Mais, cette exception ne couvre pas les données génétiques de membres de la famille de l'assuré (para.17 de la Recommandation).

. Les interdictions portent sur : 1° le traitement des données à caractère personnel relatives à la santé obtenues dans le domaine public, tels que les médias sociaux ou les forums internet, qui ne devrait pas être permis pour l'évaluation des risques ou le calcul des primes. Il s'agit d'empêcher de possibles alliances entre assureurs et acteurs de l'internet, dont certains ont déjà annoncé qu'ils allaient procédé à la collecte de données de santé. (Le magazine « New Scientist » a révélé l'existence d'un accord entre la filiale Intelligence Artificielle de Google et le NHS qui donnerait accès à cette première aux



données médicales de patients, New Scientist, Magazine issue 3072, published 7 May 2016).

2° le traitement de données à caractère personnel relatives à la santé obtenues dans le cadre d'une recherche impliquant l'assuré(e). Il s'agit de rassurer les personnes acceptant de participer à une recherche en les rassurant sur le fait que ce que la recherche a révélé sur leur santé ne puisse être utilisé au bénéfice d'un assureur. Toutefois, cette interdiction ne concerne pas « les données à caractère personnel relatives à la santé concernant tout symptôme, diagnostic, dépistage ou traitement recueilli en dehors du programme de recherche et contenu dans le dossier médical (même si elles sont en lien avec les éléments découverts grâce au programme de recherche). (Elles) peuvent être traitées si les informations satisfont aux conditions du paragraphe 5 » (Exposé des motifs, para.26). Il est à espérer que cet accès ne rendra pas l'interdiction illusoire.

B. Principe 2 : le consentement explicite de la personne

1. a) L'explicitation du principe (1^{er} alinéa)

« Les assureurs ne devraient pas procéder au traitement de données à caractère personnel relatives à la santé sans le consentement de l'assuré ».

Le caractère sensible des données personnelles de santé justifie cette disposition reprise du principe 4.6, alinéa a de la Recommandation (2002)9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance. Toutefois, s'agissant de données de santé, le texte de la présente recommandation ne prévoit pas, contrairement à l'article 4.6 b et c de la Recommandation (2002) 9, d'exceptions à l'exigence du consentement.

2. b) Les modalités de mise en œuvre (2^e alinéa)

« Les données à caractère personnel relatives à la santé devraient, en principe, être collectées par l'assureur auprès de l'assuré(e). La transmission de données à caractère personnel relatives à la santé par un tiers devrait être soumise au consentement de l'assuré(e) ».

Afin de garantir le respect du consentement explicite, le texte prévoit, conformément à l'article 4.2 de la Recommandation (2002)9, qu'en principe, il doit y avoir une transmission directe de l'assuré(e) à l'assureur. Toutefois, le texte n'interdit pas une transmission par un tiers (qui peut être le médecin de la personne concernée) mais cela suppose alors que l'assuré(e) ait donné son consentement et que l'assureur l'ait mis en mesure de vérifier si les critères permettant de justifier

sa demande (principe 1 para.5 de la Recommandation (2016)8) sont réunis.

C. « Principe 3 – Les assureurs devraient prévoir des garanties suffisantes pour la conservation des données à caractère personnel relatives à la santé ».

Il s'agit du rappel d'un des principes de base de la Convention 108 sur la protection des données énoncé à son article 5.b qui dispose que les données sont « enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités ». Il fait également référence au paragraphe 13 de la Recommandation (2002)9.

1. Paragraphe 12 : l'exigence de nécessité

Le texte ne fixe pas une limite déterminée maximale pour cette conservation mais renvoie à la notion de « nécessité pour la réalisation de l'objet pour lequel (les données) ont été collectées. A cet égard, il donne deux exemples clairs : « les données à caractère personnel relatives à la santé ne devraient pas être conservées si la demande d'assurance a été rejetée ou si le contrat est arrivé à expiration et que l'assureur n'est plus susceptible d'être appelé en garantie ». Mais, dans la réalité, il conviendra de faire une appréciation au cas par cas qui risque d'être parfois délicate. C'est pourquoi l'exposé des motifs suggère de « prendre en considération, en particulier, la nécessité de conserver des données pendant le temps nécessaire pour mener des actions en justice, fournir des preuves de transactions ou justifier une décision de refus d'accorder une assurance. Ce paragraphe prévoit néanmoins la possibilité que des données soient conservées plus longtemps si cela est requis par la loi ». (exposé des motifs n°35).

En tout état de cause, « une exemption peut être faite dans le cas où une conservation plus longue est requise par la loi » sans que le texte ne précise ici les critères de finalité et de protection de la vie privée qui rendent cette exemption légitime. On peut cependant renvoyer sur ce point à l'article 13. 1 de la Recommandation (2002)9 ainsi qu'à la jurisprudence de la Cour européenne des droits de l'homme (M. S. c. Suède (n° 20837/92) 27 août 1997 ; S. et Marper c. Royaume-Uni, arrêt (Grande Chambre) du 4 décembre 2008, § 103 ; L.H. c. Lettonie (n° 52019/07) 29 avril 2014).

2. Paragraphe 13 : règles internes de sécurité et de confidentialité

Consciente que le respect des principes et de leur mise en œuvre ne peut relever des seules autorités étatiques de régulation, dont les moyens restent limitées au



regard de l'ampleur de l'utilisation des données, la recommandation veut encourager l'auto-régulation par le développement de codes de conduite et de bonnes pratiques. Mais, elle fixe aussi quelques orientations : ainsi, « les données à caractère personnel relatives à la santé devraient être conservées avec accès limité et séparément des autres données, et les données sauvegardées à des fins de statistiques devraient être anonymisées ». Et, l'exposé des motifs explicite plus avant ces indications : . « L'accès aux données à caractère personnel relatives à la santé devrait être restreint aux personnes ayant besoin de traiter ces données en vue de l'évaluation des risques et du calcul des primes, de l'acceptation de la couverture assurantielle, ou de l'exécution d'un contrat ». . Si le contrat est échu, mais que des réclamations peuvent encore être déposées, les données ne devraient pas être conservées dans une base de données active, mais dans une base de données intermédiaire. Le paragraphe établit

en outre que les données conservées à des fins statistiques devraient être anonymisées. L'anonymisation devrait être effectuée conformément à des normes reconnues. Dans ce contexte, l'avis 05/2014 sur les techniques d'anonymisation du Groupe de travail 'Article 29' institué par la Directive 95/46/EC sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel pourrait servir de référence » (n°36).

3. Paragraphe 14 : contrôle

Afin de contrebalancer l'autonomie de régulation laissée aux assureurs, ce paragraphe « préconise l'adoption de procédures d'audit interne et externe pour veiller à ce que les règles concernant le contrôle adéquat des mesures concernant la sécurité et la confidentialité définies au paragraphe 13 de la présente Recommandation soient effectivement appliquées ». ■