UCLouvain

Faculté de droit et de criminologie

# La protection des données de santé dans le monde des assurances : enjeux et limites d'un régime juridique en construction

Éléments de droit comparé

Auteur : Oriane SCHOBER
Promoteur(s) : Geneviève SCHAMPS
Lecteur(s) : /
Année académique 2022-2023
Master Droit Finalité Justice civile et pénale

## Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

**Remerciements**

Je tiens tout d'abord à remercier chaleureusement ma promotrice de mémoire, le Professeur Schamps, pour son encadrement, ses précieux conseils et sa disponibilité.

Je remercie également son assistante, Coline Gillard, pour m'avoir aiguillée dans l'élaboration du plan de ce mémoire.

Je remercie, enfin, l'Université catholique de Louvain-La-Neuve pour son enseignement de qualité.

## Introduction

La protection des données personnelles est un enjeu crucial dans notre société numérique en constante évolution. L'avènement des nouvelles technologies de l'information et de la communication a ouvert la voie à une collecte et à un traitement massifs de données personnelles, suscitant dès lors des inquiétudes quant à la protection de celles-ci et au respect de la vie privée des individus.

Le développement à grande vitesse de l'intelligence artificielle (ci-après « IA ») confirme plus que jamais ces inquiétudes. En effet, avec l'IA, émergent de nouveaux risques de violations et de fuites de données personnelles, tels que la cybercriminalité, le traitement inapproprié de données sensibles, l'introduction de biais dans le traitement de données, et le manque de transparence. En outre, l'utilisation croissante de robots conversationnels, tels que ChatGPT, suscite des questionnements en matière de sécurité et de confidentialité des données personnelles. Selon un article du *DataNews* qui relaye une étude de la firme de sécurité Kaspersky, 42% des Belges partageraient des données professionnelles sur ChatGPT, exposant ainsi ces données à des risques de fuites[1].

Dans ce contexte, les initiatives législatives au niveau européen se multiplient pour renforcer la protection des données personnelles. Parmi les exemples récents, nous pouvons citer le nouveau cadre juridique permettant le transfert de données personnelles vers les États-Unis en toute sécurité[2]. En outre, le 4 juillet 2023, la Commission européenne dépose un projet de règlement visant à renforcer la coopération entre les autorités de protection des données et l'application du Règlement général sur la protection des données[3] (ci-après « RGPD) en établissant de nouvelles règles de procédure harmonisées afin de faire face aux défis transfrontaliers en matière de protection des données[4]. Ces exemples illustrent l'engagement constant de l'Union européenne à améliorer la sécurité des données personnelles à l'échelle européenne. Aussi, afin

[1] M. VAN DER VEN, « 42 pour cent des Belges partagent des données professionnelles avec ChatGPT », disponible sur www.datanews.levif.be, 25 juillet 2023.
[2] M. ALLO, « L'Union européenne adopte un nouveau cadre légal pour le transfert de données vers les États-Unis », disponible sur www.rtbf.be, 10 juillet 2023.
[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 36, §4 ; Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018.
[4] Commission européenne, « Protection des données : la Commission adopte de nouvelles règles pour renforcer l'application du RGPD dans les situations transfrontalières », communiqué de presse, disponible sur www.ec.europa.eu, 4 juillet 2023.

d'éviter les dérives potentielles de l'IA tout en favorisant l'innovation, l'Union européenne souhaite se doter d'un cadre juridique complet en la matière[5]. Ainsi, le 21 avril 2021, la Commission européenne dépose une proposition de règlement du Parlement européen et du Conseil, l'*IA Act*[6]. Ce règlement, actuellement en cours de discussion, prévoit des obligations pour les fournisseurs d'IA et pour leurs utilisateurs en fonction du niveau de risque que représente le système d'IA utilisé[7]. Dans la foulée, le 28 septembre 2022, la Commission européenne adopte une proposition de directive visant à établir de nouvelles règles en matière de responsabilité civile extracontractuelle applicables à l'IA[8], de sorte à protéger les consommateurs[9]. Si ces actes venaient à être adoptés, ceux-ci constitueraient les premières règles au monde sur l'IA[10].

En plus de ses nombreuses initiatives législatives, l'Union européenne surveille les pratiques des entreprises traitant des données personnelles. Ainsi, en 2022, l'Union européenne diligente des enquêtes sur l'utilisation des données personnelles par l'application chinoise TikTok, craignant des violations du RGPD par cette dernière[11]. Le 23 février 2023, la Commission européenne interdit d'ailleurs à son personnel d'utiliser l'application sur leurs appareils professionnels afin de préserver les données des instances européennes[12].

Malgré les efforts déployés pour renforcer la protection des données personnelles, les incidents de fuites et de violations de données persistent. Les géants du numérique sont particulièrement touchés. En 2021, à la suite d'une faille de sécurité, Facebook fait l'objet d'une fuite de données personnelles d'une grande ampleur. Les données personnelles de plus de 500 millions

---

[5] AFP, « Le Parlement européen veut mieux encadrer ChatGPT », disponible sur www.lesoir.be, 11 mai 2023.
[6] Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM (2021) 206 final, 21 avril 2021.
[7] Parlement européen, « Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle », disponible sur www.europarl.europa.eu, 9 juin 2023.
[8] Proposition de directive du Parlement européen et du Conseil relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle (directive sur la responsabilité en matière d'IA), COM (2022) 496 final, 28 septembre 2022.
[9] Commission européenne, « De nouvelles règles en matière de responsabilité applicables aux produits et à l'IA pour protéger les consommateurs et favoriser l'innovation », disponible sur www.france.representation.ec.europa.eu, 28 septembre 2022.
[10] Parlement européen, « Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle », disponible sur www.europarl.europa.eu, 9 juin 2023.
[11] J. RAGOT, « TikTok : l'Union européenne lance plusieurs enquêtes sur l'usage des données personnelles par la Chine », disponible sur www.bfmtv.com, 23 novembre 2022.
[12] AFP, « Les institutions européennes veulent interdire TikTok à leurs personnels pour « protéger » leurs données », disponible sur www.rtl.be, 23 février 2022.

d'utilisateurs se sont retrouvées en libre accès sur Internet[13]. Plus récemment encore, au début de l'année 2023, le réseau social Twitter fait l'objet d'une fuite massive de données personnelles à la suite à d'un dysfonctionnement de l'API de la plateforme. 235 millions d'adresses électroniques d'utilisateurs se sont alors retrouvées sur un forum de hackers, créant ainsi un risque d'importantes escroqueries en ligne[14]. Force est de constater que les exemples de fuites de données massives sont nombreux. En tout état de cause, ces incidents soulignent l'urgence d'établir un régime de protection efficace des données personnelles, et surtout de veiller à son application concrète.

Si la protection des données personnelles est un enjeu crucial, la protection des données de santé revêt une importance plus cruciale encore, ces données étant qualifiées de sensibles. La pandémie de la Covid-19 met en évidence les risques de violation des données de santé. Outre la problématique de la légalité des réglementations prises au début de la crise, de nombreuses dispositions impliquant le traitement et l'échange de données de santé sont adoptées dans le cadre de la pandémie. Bien que la situation nécessite une réaction urgente de part du gouvernement belge, l'Autorité de protection des données (ci-après l'APD) déplore que bon nombre des initiatives réglementaires sont prises sans que cette dernière ne soit consultée, cette consultation étant pourtant une obligation légale[15]. Celle-ci est dès lors empêchée de contrôler le respect, par ces réglementations, des normes en matière de protection des données et de la vie privée[16].

Ces éléments d'actualité constituent un point de départ pertinent pour démontrer d'une part, la fragilité des données de santé et d'autre part, l'urgence de renforcer le cadre existant et son effectivité.

Le paradoxe d'un régime juridique strict avec des situations de violations structurelles est particulièrement bien illustré dans le cas des assurances. C'est pour cela que nous allons nous

[13] H. BOUNEMOURA, « Facebook : Tout comprendre à la fuite de données qui concerne 533 millions d'utilisateurs », disponible sur www.20minutes.fr, 7 avril 2021.
[14] M. LE PRIOL, « Twitter : fuite de données personnelles d'une ampleur inédite pour la plateforme », disponible sur www.la-croix.com, 6 janvier 2023.
[15] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 36, §4 ; Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 23.
[16] Autorité de protection des données, « Lettre aux parlements et gouvernements belges », disponible sur www.autoriteprotectiondonnees.be, 2 février 2021, p. 2.

intéresser, dans le cadre de ce mémoire, aux enjeux et aux limites de la protection des données de santé par les assurances, s'agissant d'un régime en construction, directement inscrit dans son contexte.

Ainsi, ce mémoire tentera de répondre aux interrogations suivantes : **quels sont les mécanismes de protection des données de santé actuels ? De quelle façon les assurances sont-elles soumises à l'obligation d'une protection renforcée des données de santé ? Quelles sont les limites – théoriques et pratiques – de cette protection renforcée ?**

Pour répondre aux différentes problématiques de ce sujet, nous avons mobilisé différentes sources et méthodologies. En ce qui concerne les sources et la bibliographie, dans un premier temps, nous avons mobilisé les sources juridiques « officielles », *i.e.* législations, règlements, directives, jurisprudence et doctrine. Pour apporter une hauteur contextuelle, nous avons également accordé une place centrale à la presse écrite. Par ailleurs, pour pallier le manque de sources doctrinales, de nombreuses sources proviennent sont non officielles (guidelines, articles de presse, etc.) postées sur Internet. Elles sont de fiabilité variable et une certaine vigilance à leur égard est de mise, bien que nous ayons procédé à la vérification des informations dans la mesure du possible. Quant aux méthodologies utilisées, nous allons emprunter un point de vue macro- et micro- pour exposer les complexités et les ambiguïtés sous-jacentes liées à la question de la protection des données de santé par les assurances. Nous inspirant des méthodes de sciences sociales, nous avons procédé à des entretiens. Nous avons ainsi eu l'occasion d'interroger l'ancien responsable des assurances de Tests-Achats, ainsi qu'un médecin généraliste[17]. Enfin, au sein de ce mémoire, nous allons également mettre en avant des éléments de droit comparé, visant à illustrer des difficultés liées à la protection des données de santé.

Ce mémoire est divisé en deux parties. Une première partie sera consacrée à l'étude du régime des données de santé en lien avec les assurances (point de vue macro). Nous verrons qu'il s'agit d'un régime constitué de nombreuses réglementations éparses, rendant ainsi difficile son appréhension de manière exhaustive (**chapitre 1**). Une deuxième partie sera consacrée à l'étude de trois cas-limites (point de vue micro) : le recours à des détectives privés par les compagnies d'assurance, le cas spécifique de la médecine d'assurance, et enfin, les défis d'aujourd'hui et de demain concernant les données recueillies par les objets connectés (**chapitre 2**).

[17] Pour des raisons de confidentialité, ces entretiens n'ont pas été reproduits en annexe du présent mémoire. Les propos des personnes interviewées seront utilisés dans leur généralité pour illustrer un argumentaire.

## Chapitre 1. Une étude générale du régime de traitement des données de santé en lien avec les assurances dans le droit belge

Afin de comprendre les enjeux du régime de la protection des données de santé en lien avec les assurances, il nous paraît nécessaire d'historiciser un tel régime afin d'avoir un aperçu général de la construction de la spécificité des données de santé (**section 1.**). Nous nous attarderons ensuite sur la relation ambiguë qu'entretiennent les assurances avec le nouveau régime de protection des données de santé (**section 2.**).

### Section 1. Une historicisation du régime spécifique du traitement des données de santé : des lois nationales au RGPD

Au sein de cette Section, nous étudierons l'histoire du régime de protection des données, des lois nationales au RGPD, afin de comprendre la spécificité de la protection des données de santé dans le droit belge et leur traitement par les assurances (**§1**). Nous nous attarderons ensuite sur le rôle d'une autorité de protection des données qui s'impose difficilement dans l'horizon juridique belge (**§2**).

#### §1. Des lois nationales au RGPD : une gestation longue et laborieuse du régime de protection des données de santé belge par rapport à d'autres États membres

En Belgique, le premier projet de loi visant à protéger la vie privée à l'égard des banques de données est déposé le 8 avril 1976. Ainsi, après la Suède, la Belgique est le premier pays à soumettre une réglementation des écoutes et des traitements de données, étant dès lors considérée comme la pionnière de la protection de la vie privée. Ce projet n'est toutefois pas adopté[18]. Quinze ans plus tard, en 1991, la Belgique ne dispose toujours pas de législation générale en la matière[19], faisant d'elle paradoxalement, avec l'Irlande, le dernier pays de l'Europe des Douze à en être dénué[20]. En effet, entre-temps, des pays comme l'Allemagne ou

[18] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, rapport fait au nom de la commission de la justice, *Doc., Ch*., 1991-1992, n°413/12, p. 3.
[19] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, exposé des motifs, *Doc., Ch*., 1990-1991, n°1610/1, p. 1.
[20] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, rapport fait au nom de la commission de la justice, *Doc., Sén*., 1992-1993, n°445/2, p. 3.

la France se dotent d'un arsenal juridique important, considéré comme primordial dans la constitution d'un régime de protection des données, aux échelles européenne et internationale.

Pour revenir au cas belge, le 7 mai 1982, l'État signe la Convention n°108 du Conseil de l'Europe du 28 janvier 1981 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[21] entrant en vigueur le 1er octobre 1985. Cette convention constitue la première tentative d'harmonisation en la matière, mais n'aboutit pas à une protection équivalente dans tous les États membres de la Communauté[22]. Ratifiée par une loi du 17 juin 1991[23], elle devient le fondement de la loi ultérieure du 8 décembre 1992[24]. Les travaux préparatoires de la loi du 8 décembre 1992 évoquent l'urgence d'adopter une législation générale en la matière, au risque pour la Belgique de se retrouver isolée de ses principaux partenaires politiques et économiques qui, dotés telle d'une législation, deviennent de plus en plus réticents à transférer des données à caractère personnel vers un pays dénué de toute protection en la matière, pouvant ainsi constituer un frein au bon développement d'un marché européen de l'information[25]. En raison de l'absence d'une législation générale en la matière, la Belgique est peu à peu isolée sur la scène internationale[26]. Par ailleurs, les accords de Schengen conditionnant leur entrée en vigueur par l'existence d'une loi générale dans chaque État membre, l'absence d'une telle législation permet aux multinationales de s'établir en Belgique pour échapper à la réglementation, provoquant ainsi le mécontentement des États voisins[27].

D'autre part, l'importance et la nécessité d'une législation spécifique en la matière s'expliquent par l'avènement de l'informatisation qui, bien que contribuant à une meilleure organisation de l'administration et au développement de l'économie, présente des dangers. En effet, en raison

[21] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, conclue au sein du Conseil de l'Europe le 28 janvier 1981, *S.T.C.E.*, n°108.
[22] Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, rapport fait au nom de la commission de la justice, *Doc., Ch.*, 1998-1999, n°1566/10, p. 4.
[23] Loi du 17 juin 1991 portant approbation de la convention relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, *M.B.*, 30 décembre 1993.
[24] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.
[25] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, exposé des motifs, *Doc., Ch.*, 1990-1991, n°1610/1, p. 2.
[26] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, rapport fait au nom de la commission de la justice, *Doc., Ch.*, 1991-1992, n°413/12, p. 4.
[27] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, rapport fait au nom de la commission de la justice, *Doc., Ch.*, 1991-1992, n°413/12, p. 5.

du nombre croissant de données, les liaisons et les interconnexions sont plus faciles à réaliser, de sorte que des accès illicites et des abus peuvent en résulter[28]. La loi du 8 décembre 1992[29] pose dès lors les principes généraux en matière de protection de la vie privée qui s'imposeront à toutes les banques de données, tant dans le secteur privé que public. Cette loi concerne uniquement le traitement (automatisé ou manuel) des données à caractère personnel qui est en principe autorisé, mais subordonné au respect de certaines conditions, à la reconnaissance de droits et d'obligations corrélatives, et qui ne peut avoir lieu que pour des finalités déterminées et légitimes[30]. Concernant les données sensibles, comme les données médicales, les conditions sont plus strictes. Les données médicales ne peuvent en effet être traitées que sous la surveillance et la responsabilité d'un praticien de l'art de guérir, sauf consentement écrit de la personne concernée[31].

Surtout, c'est l'accaparement par le droit de l'Union européenne de cette problématique qui pose les nouvelles bases de la protection des données à l'échelle européenne. En effet, en 1995, l'Union européenne adopte la directive de protection des données 95/46/CE[32] afin d'harmoniser les législations nationales en la matière, et de faciliter, au sein de la Communauté, la libre circulation et l'échange des données générées par la réalisation du marché intérieur. Afin de supprimer les obstacles qui entravent la libre circulation des données à caractère personnel, le niveau de protection des droits et libertés des personnes à l'égard du traitement de celles-ci doit être équivalent dans tous les États membres[33]. L'adoption de cette directive est déjà motivée par la nécessité d'avoir un cadre juridique clair et stable, indispensable pour le développement de la société de l'information et la protection des citoyens européens à cet égard[34].

---

[28] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, rapport fait au nom de la commission de la justice, *Doc., Sén*., 1992-1993, n°445/2, p. 4.
[29] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B*., 18 mars 1993.
[30] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, exposé des motifs, *Doc., Ch*., 1990-1991, n°1610/1, p. 4.
[31] T. LEONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution – La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995 », *J.T*., n°20, 1999, p. 377 à 396.
[32] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E*., L281, 23 novembre 1995.
[33] Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, rapport fait au nom de la commission de la justice, *Doc., Ch*., 1998-1999, n°1566/10, p. 4 et 5.
[34] Avis de la Commission des Communautés européennes concernant la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, COM (1995) 375 final, 18 juillet 1995, p. 2.

En vertu de l'article 32 de la directive, les États membres doivent transposer cette directive au plus tard le 24 octobre 1998[35]. En Belgique, cette transposition résulte, d'une part, de l'adaptation de la loi du 8 décembre 1992 et d'autre part, par l'entrée en vigueur d'une nouvelle loi du 11 décembre 1998[36].

La loi du 11 décembre 1998 remanie profondément le régime des données médicales. En effet, il désormais question de données relatives à la santé[37]. Alors que précédemment les données médicales désignaient « toutes données à caractère personnel dont nous pouvons déduire une information sur l'état antérieur, actuel ou futur de la santé physique ou psychique, à l'exception des données purement administratives ou comptables relatives aux traitements et aux soins médicaux »[38], le nouvel article 7 de la loi ne définit plus ce qu'il faut entendre par ce type de données. L'exposé des motifs invite à reconnaître une portée plus étroite à la donnée relative à la santé en excluant les données qui révèlent seulement l'état de santé d'un individu mais qui ne se rapportent pas à sa santé. L'article 7 interdit en principe le traitement de données relatives à la santé, tout en prévoyant un très grand nombre d'exceptions, comme le consentement écrit de la personne concernée, le traitement nécessaire à l'exécution d'obligations issues du droit du travail, ou encore le traitement nécessaire à l'application de la sécurité sociale. Ces exceptions ne sont admises que si les traitements des données relatives à la santé sont effectués sous la responsabilité d'un professionnel des soins de santé, sauf en cas de consentement de la personne concernée ou de nécessité pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée[39]. Le nouvel article 7 ne permet toutefois pas de déterminer avec précision qui sont ces professionnels des soins de santé. En outre, en vertu du paragraphe 5 de l'article 7, les données relatives à la santé ne peuvent être collectées qu'auprès de la personne concernée afin de lui permettre de contrôler les communications de ses données. Par exception, les données relatives à la santé ne peuvent être collectées auprès d'autres sources qu'au moyen du respect des conditions prescrites par la disposition : la collecte doit être conforme aux

[35] Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, exposé des motifs, *Doc., Ch*., 1997-1998, n°1566/1, p. 3.
[36] Loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B*., 3 février 1999.
[37] Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, rapport fait au nom de la commission de la justice, *Doc., Ch*., 1998-1999, n°1566/10, p. 13.
[38] T. LEONARD et Y. POULLET, *op. cit*., p. 377 à 396.
[39] T. LEONARD et Y. POULLET, *ibidem*, p. 377 à 396.

conditions prescrites par le Roi, être effectuée sous la responsabilité du professionnel des soins de santé, et être nécessaire à la finalité poursuivie[40].

La loi du 8 décembre 1992 est finalement abrogée par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel[41], entrée en vigueur le 5 septembre 2018, qui implémente et complète le RGPD, entré en vigueur le 25 mai 2018, qui remplace la directive 95/46/CE.

À la suite de la directive 95/46/CE, le RGPD marque un nouveau tournant dans la clarification et le renforcement du régime de la protection des données à caractère personnel. L'entrée en vigueur du RGPD s'explique pour des raisons contextuelles mais aussi structurelles ou institutionnelles. En effet, le RGPD intervient plus de 20 ans après la directive, alors que l'utilisation des technologies numériques dans la vie privée explose. La directive 95/46/CE est mise en œuvre alors qu'Internet est encore à ses balbutiements et que le traitement et le partage de données n'est pas aussi répandus qu'ils le sont aujourd'hui. La directive vise à fournir une norme minimale pour la protection des données dans l'ensemble de l'Union européenne, mais est mise en œuvre différemment dans chaque État membre de l'Union européenne. Cela conduit à des incohérences et à de la confusion concernant les réglementations en matière de protection des données et leur application. Par ailleurs, le recours à l'instrument réglementaire plutôt qu'à la directive s'explique par le fait de ne pas dénaturer à outrance les dispositions du Règlement, même si celui-ci laisse une place importante à la marge de manœuvre des États membres[42]. Un règlement censé s'appliquer de façon plus ou moins uniforme va davantage dans le sens d'une harmonisation des ordres juridiques nationaux en la matière[43]. Rapidement, le RGPD s'est imposé comme une référence en matière de protection des données personnelles au niveau

[40] T. LEONARD et Y. POULLET, *op. cit*., p. 377 à 396.
[41] Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B*., 5 septembre 2018.
[42] A. ROSSOW, « The Birth of GDPR : What Is It And What You Need To Know », disponible sur www.forbes.com, 25 mai 2018.
[43] M. BURGESS, « What is GDPR ? The summary guide to GDPR compliance in the UK », disponible sur www.wired.co.uk, 24 mars 2020 ; N. LORD, « What is the Data Protection Directive ? The Predecessor to the GDPR », disponible sur www.digitalguardian.com, 28 décembre 2022.

européen et au niveau international[44], inspirant par exemple le *California Consumer Privacy Act*[45].

Le RGPD se caractérise par la mise en place d'une logique de responsabilisation importante à l'égard des responsables de traitement de données à caractère personnel. Par ailleurs, il met également à disposition des autorités de protection des données compétentes un cadre de sanctions précises, contrairement à la directive, ce qui est une garantie de son effectivité[46]. Enfin, nous concernant, l'une des plus grandes avancées du RGPD concerne la reconnaissance de la spécificité des données dites « sensibles ». En effet, les données dites « sensibles », au rang desquelles figurent les données de santé, font l'objet d'un régime de protection spécial en raison du risque accru de discriminations auxquelles peut donner lieu leur exploitation, et de leur forte proximité avec l'intimité des personnes concernées[47]. L'article 9, §1 du RGPD interdit donc en principe leur traitement.

Comme nous l'avons précisé, l'article 4, §15 du RGPD définit les données concernant la santé comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne »[48]. Le considérant 35 du RGPD vient compléter cette définition en indiquant que « les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée, comme toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé,

[44] E. THELISSON, « La portée du caractère extraterritorial du Règlement général sur la protection des données », *Revenue internationale de droit économique*, 2019, t. XXXIII, n°4, p. 16.
[45] M. BURGESS, « What is GDPR ? The summary guide to GDPR compliance in the UK », disponible sur www.wired.co.uk, 24 mars 2020 ; N. LORD, « What is the Data Protection Directive ? The Predecessor to the GDPR », disponible sur www.digitalguardian.com, 28 décembre 2022.
[46] M. KHELOUFI, « Entrée en vigueur du règlement général sur la protection des données : le changement dans la continuité », disponible sur www.revue-jade.eu, 30 octobre 2019.
[47] J.-M. VAN GYSEGHEM, « Les catégories particulières de données à caractère personnel », *Le règlement général sur la protection des données (RGPD/GPDR) – Analyse approfondie*, C. de Terwangne et K. Rosier (dir.), Collection du CRIDS, Bruxelles, Larcier, 2018, p. 255.
[48] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 4, §15.

d'un hôpital, d'un dispositif médical ou d'un test de diagnostic *in vitro* »[49]. Mais avant même le RGPD, les données de santé reçoivent une attention accrue de la part des acteurs juridiques. Ainsi, dans un arrêt du 6 novembre 2003, la Cour de justice de l'Union européenne (ci-après « CJUE ») indique que la notion de données relatives à la santé doit recevoir une interprétation large, de sorte qu'elle comprend les informations portant sur « tous les aspects, tant physiques que psychiques, de la santé d'une personne »[50]. Dans un avis du 15 février 2007, le Groupe 29 estime que les données relatives à la santé incluent les données présentant « un lien clair et étroit avec la description de l'état de santé d'une personne »[51], comme la consommation de médicaments, d'alcool ou de drogues.

Bien que la protection soit accrue en matière des données de santé, elle n'est pas pour autant absolue. En effet, par dérogation au principe, l'article 9, §2 du RGPD prévoit un certain nombre d'hypothèses dans lesquelles les données sensibles peuvent être traitées, comme le consentement explicite de la personne concernée et la nécessité du traitement pour l'exécution d'obligations en matière de sécurité et de protection sociales ou la gestion d'un système de soins de santé. Enfin, il importe de rappeler que si les assureurs, responsables de traitement que nous privilégions dans notre étude, peuvent se fonder sur les bases de licéité de l'article 9, §2 du RGPD pour traiter, par exception au principe, des données sensibles telles que les données concernant la santé, ces derniers doivent toutefois respecter les principes de base de la protection des données énoncés par l'article 5 du RGPD (*voy*. Section 2)[52].

Ce Paragraphe a eu vocation à exposer une brève histoire de la protection des données personnelles dans le droit belge. De façon générale, ce paragraphe démontre également, en filigrane, l'évolution dans les enjeux de la protection des données à caractère personnel. En effet, dans les années 1970, l'opinion publique se méfie fortement de l'informatisation de la société et des risques liés aux abus, mais qui émaneraient des autorités publiques. Depuis les années 1990, les enjeux concernent la protection des données à caractère personnel du fait du développement exponentiel d'un usage personnel et individuel des outils informatiques et

[49] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, considérant 35.
[50] C.J.C.E., arrêt *Lindqvist*, 6 novembre 2003, C-101/01, EU:C:2003:596, point 50.
[51] Groupe de travail « article 29 » sur la protection des données, « Document de travail sur le traitement des données relative à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME) », WP 131, disponible sur www.ec.europa.eu, 15 février 2007, p. 8.
[52] J.-M. BINON, « Assurances de personnes et protection des données personnelles : un mariage tumultueux à l'ombre du RGPD », *R.D.C.*, 2021/9, p. 1964.

technologiques, s'accompagnant par la fragilisation de ces individus face à des acteurs privés tels que les GAFA ou les compagnies d'assurance[53]. Enfin, nous comprenons désormais que, en Belgique, la mise en place d'une telle protection a été longue, arrivant relativement tard au sein de l'Union européenne. En ce sens, l'adoption du RGPD est bienvenue et la tentative d'harmonisation des régimes juridiques européens en la matière a semblé nécessaire au législateur européen.

## §2. Le rôle de l'Autorité de protection des données de santé : un rôle fragilisé dans un contexte de remise en cause de sa légitimité

Une analyse du régime juridique de la protection des données mérite d'être combinée avec l'étude des autorités de contrôle indépendantes, lesquelles sont chargées du bon respect de cette protection et donc de son effectivité. Ainsi, en Europe, la naissance des premières autorités de contrôle remonte aux années 1970, et est liée à la méfiance à l'égard de l'administration qui s'est informatisée[54]. Les autorités de contrôle sont dès lors chargées de contrôler l'accès aux premières bases de données étatiques afin d'empêcher des abus dans l'utilisation des données à caractère personnel. La Commission consultative de la protection de la vie privée instituée en 1983 lors de la création du Registre national afin d'empêcher un usage abusif de cette première base de données étatique est la première autorité de ce genre. La directive 95/46/CE impose déjà à chaque État membre de se doter d'une ou plusieurs autorités de contrôle, mais leur laisse une marge de manœuvre en ce qui concerne, notamment, leur statut, leur mode de fonctionnement, et les ressources mises à leur disposition[55]. Cette marge de manœuvre laissée aux États membres entraine des disparités entre les différentes autorités de contrôle européennes. Ainsi, par exemple, le législateur belge n'a pas doté la Commission de la vie privée, devenue aujourd'hui l'APD, du pouvoir de sanction, contrairement aux autres autorités de contrôle européennes[56].

[53] A. DEVILLARD, « Sous Giscard, la création de la Cil après un "SAFARI" », disponible sur www.sciencesetavenir.fr, , 4 décembre 2020.
[54] E. DEGRAVE, « L'autorité de contrôle », *Le règlement général sur la protection des données (RGPD/GPDR) – Analyse approfondie*, C. de Terwangne et K. Rosier (dir.), Collection du CRIDS, Bruxelles, Larcier, 2018, p. 593.
[55] E. DEGRAVE, *ibidem*, p. 596.
[56] E. DEGRAVE, *ibidem*, p. 597.

Le RGPD entend dès lors harmoniser les différentes autorités de contrôle européennes et cela se reflète dans son considérant 129[57]. Pour aller dans le sens de l'harmonisation, les missions et pouvoirs de l'autorité de contrôle sont énoncés de manière bien plus précise aux articles 57 et 58 du RGPD que dans la directive 95/46/CE, et chaque autorité de contrôle doit désormais être investie d'un pouvoir de sanction défini et organisé par l'article 83 du RGPD[58]. Il renforce par ailleurs l'exigence d'indépendance des autorités de contrôle[59], et encourage fortement la coopération entre ces dernières afin que le droit européen de la protection des données soit mis en œuvre de manière plus uniforme au sein de l'Union européenne[60]. Aussi, à la suite de ces évolutions, l'APD devient la nouvelle autorité de contrôle belge qui remplace la Commission pour la protection de la vie privée instituée en 1992 à la suite de la directive 95/46/CE. L'APD est créée par une loi du 3 décembre 2017[61] afin de se mettre en conformité avec les nouvelles exigences du RGPD[62].

L'APD est une autorité administrative indépendante dotée de la personnalité juridique, en vertu de laquelle elle peut ester en justice pour dénoncer une violation des principes fondamentaux de la protection des données à caractère personnel et pour faire appliquer ces derniers, et être attraite en justice[63]. Elle est composée de six organes, à savoir d'un comité de direction composé des directeurs des autres organes, d'un secrétariat général, d'un service de première ligne, d'un centre de connaissance, d'un service d'inspection, et d'une chambre contentieuse[64]. Elle est chargée de veiller au respect des règles de la protection des données à caractère personnel. À cet égard, elle dispose de pouvoirs d'investigation, d'autorisations préalables, de saisie, de mise sous scellé, ainsi que d'un arsenal de sanctions allant du simple avertissement à des amendes administratives pouvant aller jusqu'à vingt millions d'euros ou quatre pourcents du chiffre

[57] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, considérant 129.
[58] E. DEGRAVE, *op. cit.*, p. 598.
[59] E. DEGRAVE, « Le RGPD, les lois belges et le secteur public – Les traitements de données dans l'administration en réseaux et l'Autorité de protection des données », *Le règlement général sur la protection des données (RGPD/G.D.P.R.) : premières applications et analyse sectorielle*, H. Jacquemin (dir.), Commission Université – Palais – Université de Liège, Liège, Anthemis, 2020, vol. 195, p. 308.
[60] M.-H. BOULANGER, « Quelques remarques sur les autorités indépendantes de protection des données dans l'ordre juridique européen », *Le règlement général sur la protection des données (RGPD/GPDR) – Analyse approfondie*, C. de Terwangne et K. Rosier (dir.), Collection du CRIDS, Bruxelles, Larcier, 2018, p. 487 et 488.
[61] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018.
[62] E. DEGRAVE, « Le RGPD, les lois belges et le secteur public – Les traitements de données dans l'administration en réseaux et l'Autorité de protection des données », *op. cit.*, p. 308.
[63] E. DEGRAVE, « L'Autorité de protection des données, un nouveau chien de garde de la vie privée des citoyens », disponible sur www.justice-en-ligne.be, 8 janvier 2020.
[64] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 7.

d'affaires annuel mondial d'une entreprise[65]. *Via* son centre de connaissances, elle joue également un rôle de prévention dans l'élaboration des normes sur les données à caractère personnel et la vie privée. En effet, lorsqu'une loi, une ordonnance ou un décret sont adoptés en matière de données à caractère personnel, l'autorité publique à l'origine de cette norme est obligée de demander à l'APD de rendre un avis sur celle-ci afin de s'assurer qu'elle est conforme à la réglementation relative à la protection des données et de la vie privée[66].

Pour qu'une autorité de contrôle puisse jouer de manière effective son rôle de gardienne de la vie privée, elle se doit d'être indépendante des responsables de traitement publics et privés qu'elle contrôle. Cela est rappelé à trois reprises par la CJUE[67]. L'indépendance de l'APD se traduit tout d'abord au niveau institutionnel en octroyant à l'autorité les ressources financières et matérielles nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, et en veillant à ce qu'elle ne soit pas soumise à une subordination hiérarchique, tel qu'un contrôle de tutelle exercé par l'État[68]. D'autre part, son indépendance est surtout celle de ses membres[69]. En effet, « le ou les membres de chaque autorité de contrôle demeurent libres toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions de quiconque »[70] et « s'abstiennent de tout acte ou activité professionnelle incompatibles avec leurs fonctions »[71]. Les articles 43 et 44 de la loi portant création de l'APD précisent que par activité incompatible, il faut entendre « une activité pouvant bénéficier directement ou indirectement des décisions et prises de position que peut prendre l'[APD] »[72]. L'indépendance des membres de l'autorité est intrinsèquement liée au mode de désignation de ceux-ci. En Belgique, les membres de l'APD

[65] E. DEGRAVE, « Le RGPD, les lois belges et le secteur public – Les traitements de données dans l'administration en réseaux et l'Autorité de protection des données », *op. cit*., p. 310 à 312.
[66] E. DEGRAVE, « La compétence d'avis de l'Autorité de protection des données : une aide précieuse dans l'élaboration des normes sur les données à caractère personnel et la vie privée », disponible sur www.justice-en-ligne.be, 10 décembre 2021.
[67] C.J., arrêt *Commission c. Hongrie*, 8 avril 2014, C-288/12, EU:C:2014:237 ; C.J., arrêt *République d'Autriche c. Commission*, 16 octobre 2012, C-614/10, EU:C:2012:605 ; C.J., arrêt *République fédérale d'Allemagne c. Commission*, 9 novembre 2010, C-518/07, EU:C:2010:125.
[68] E. DEGRAVE, « L'autorité de contrôle », *op. cit*., p. 605.
[69] E. DEGRAVE, « L'autorité de contrôle », *ibidem*, p. 601.
[70] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E*., L119, 4 mai 2016, art. 52, §2.
[71] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E*., L119, 4 mai 2016, art. 52, §3.
[72] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B*., 10 janvier 2018, art. 44, §1 ; E. DEGRAVE, « Le RGPD, les lois belges et le secteur public », *Le Règlement général sur la protection des données (RGPD/G.D.P.R.) : premières applications et analyse sectorielle*, H. Jacquemin (dir.), Anthemis, Liège, 2020, p. 308 à 317.

sont élus par la Chambre des représentants à la majorité simple[73]. Dans les travaux préparatoires de la loi du 3 décembre 2017, certains soutiennent que les membres devraient être élus à la majorité spéciale afin de renforcer la voix de l'opposition dans le débat. Cela n'est toutefois pas retenu lors de l'adoption de la loi[74].

Cette indépendance est donc essentielle pour que cette dernière puisse examiner et déterminer, de manière objective et impartiale, l'équilibre à atteindre entre la circulation des données à caractère personnel et la protection de vie privée, et ainsi faire respecter le régime juridique de la protection des données[75]. Toutefois, en juin 2021, la Belgique fait l'objet d'une procédure pour infraction grave au RGPD en raison de la non-indépendance de son autorité de contrôle. En effet, le 9 juin 2021, la Commission européenne annonce avoir ouvert, à l'encontre de la Belgique, une procédure pour infraction grave au RGPD à la suite d'une plainte anonyme, déposée en novembre 2020 auprès du Commissaire Didier Reynders, qui dénonce l'existence de mandats illégaux au sein l'APD. Il est alors reproché à quatre membres de l'APD d'exercer des activités incompatibles avec leur mandat, à savoir des mandats publics. La Belgique est le premier État à faire l'objet d'une telle procédure depuis l'adoption du RGPD[76]. La Commission considère que la Belgique viole l'article 52, paragraphes 1, 2 et 3 du RGPD « dès lors que certains membres de l'APD ne demeuraient pas libres de toute influence extérieure ; exerçaient des activités professionnelles incompatibles et que le défaut d'indépendance de certains de ses membres affectait l'indépendance de l'exercice des missions et pouvoirs de l'APD dans son ensemble ». À la suite de la démission de deux des quatre membres, les membres restants demeurent problématiques pour la Commission européenne, s'agissant de Bart Preneel (cryptologue de la KULeuven, membre externe de l'APD et membre du Comité de sécurité de l'information) et Frank Robben (administrateur général de la Banque Carrefour de la Sécurité sociale, de la plateforme eHealth, patron de la Smals, principal rédacteur des décisions du Comité de sécurité de l'information et membre externe de l'APD). Il leur est reproché d'être à la fois juges et parties. Le 12 novembre 2022, la Commission européenne adresse une lettre de mise en demeure à la Belgique dans laquelle elle somme cette dernière de prendre les mesures appropriées pour mettre fin aux irrégularités dans un délai de deux mois à compter de sa

[73] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 36 et *s*.
[74] M.-H. BOULANGER, *op. cit*., p. 604 et 605.
[75] E. DEGRAVE, « L'autorité de contrôle », *op. cit*., p. 599.
[76] BELGA, « RGPD : la Commission européenne ouvrira une procédure d'infraction contre la Belgique », disponible sur www.rtbf.be, 9 juin 2021.

réception. Au dernier jour du délai, le gouvernement belge adresse un courrier à la Commission européenne, mais ne règle pas entièrement le problème[77]. En effet, après plus d'un an de discussions en commission de la justice, le Parlement décide, mi-décembre, de lancer une procédure de levée de mandat, conformément à l'article 45 de la loi portant création de l'APD, contre David Stevens (président de l'APD) et Charlotte Dereppe. David Stevens est notamment soupçonné de conflits d'intérêts pour avoir participé au début de la pandémie à la Task force « Data against corona ». Quant à Charlotte Dereppe, il lui est en grande partie reproché son absence aux réunions du comité de direction et donc de ne plus remplir les conditions d'éligibilité[78]. Les mandats de Frank Robben et de Bart Preneel sont quant à eux maintenus, de sorte que la Belgique est menacée d'être attraite devant la CJUE.

En janvier 2022, un projet de réforme de l'APD est entrepris par Mathieu Michel, le secrétaire d'État à la digitalisation. Cette réforme vise à renforcer le fonctionnement, l'expertise et l'indépendance de l'APD. Les principaux éléments clés de la réforme sont les suivants : la transformation du comité de direction en un organe collégial, l'octroi à l'APD d'une plus grande marge de manœuvre dans son fonctionnement interne, la compétence exclusive de l'APD pour exercer les missions et mandats du contrôle du respect de la mise en œuvre du RGPD, ainsi que le renforcement des règles d'incompatibilité et de conflit d'intérêt[79]. Toutefois, le projet de loi essuie beaucoup de critiques de la part d'une frange de la société civile et d'académiques qui craignent que cette réforme rende davantage l'APD dépendante de ceux qu'elle est censée contrôler[80]. Dans un avis du 25 février 2022, l'APD soutient que cette réforme mettrait gravement en péril son efficacité et son indépendance, et demande dès lors qu'il soit remédié aux manquements qu'elle a identifié dans son avis[81]. Quant à l'opposition, elle soutient que le texte comporte toujours une série d'inconstitutionnalités et qu'aucune modification n'a été apportée par la majorité[82] après déjà quatre passages en plénière, trois passages par le Conseil

[77] P. LALOUX, « Pourquoi le problème de non-indépendance de l'APD est loin d'être réglé », disponible sur www.lesoir.be, 14 janvier 2022.
[78] P. LALOUX, « Pourquoi le problème de non-indépendance de l'APD est loin d'être réglé », disponible sur www.lesoir.be, 14 janvier 2022.
[79] SPF Chancellerie du Premier Ministre – Direction générale Communication externe, « Renforcement de l'indépendance et du fonction de l'Autorité de protection des données – Deuxième lecture », disponible sur www.news.belgium.be, 24 juin 2022.
[80] P. LALOUX, « Critiqué, torpillé, saboté… le projet de loi APD de Mathieu Michel va une nouvelle fois se faire recaler », disponible sur www.lesoir.be, 2 février 2023.
[81] Autorité de protection des données, « Avis concernant un avant-projet de loi modifiant la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (AH-2022-0020), disponible sur www.autoriteprotectiondonnees.be, 25 février 2022.
[82] BELGA, « Vie privée sous tension – Le projet de loi réformant l'APD renvoyé une nouvelle fois au Conseil d'État », disponible sur www.lalibre.be, 30 mars 2023.

d'État et une note légistique des services de la Chambre. À l'heure actuelle, le projet de loi n'a toujours pas été adopté, et de nouveaux amendements ont été déposés par l'opposition. Ceux-ci seront prochainement examinés par le Conseil d'État[83].

Le 26 janvier 2023, la Commission européenne initie de nouveau une procédure d'infraction contre la Belgique, cette fois-ci au sujet de la révocation des mandats de David Stevens et de Charlotte Dereppe au motif qu'elle est contraire au droit européen[84]. Charlotte Dereppe dénonce d'ailleurs les conditions de sa procédure de révocation au Parlement (huis clos, absence de faute grave, etc.) auprès de la Commission européenne, en violation de l'article 53, §4 du RGPD. Par ailleurs, au moment de la révocation de Charlotte Dereppe, la directive sur la protection des lanceurs d'alerte[85] n'est pas transposée en droit belge. Cette dernière prévoit une protection contre les représailles lorsqu'un lanceur d'alerte signale une infraction à une réglementation. Le Parlement national considère que la révocation de Charlotte Dereppe n'est pas liée à son alerte, avec pour conséquence qu'elle ne peut bénéficier de la protection liée au statut de lanceur de l'alerte. Elle introduit dès lors un recours devant le Tribunal de première instance afin que ce statut lui soit reconnu[86]. Après un long processus, la directive est *in fine* transposée en Belgique par une loi du 28 novembre 2022[87].

Le 7 février 2022, à la veille du dépôt de plainte par la Commission à la CJUE, Frank Robben envoie sa lettre de démission, ce qui évite de justesse à la Belgique un passage devant la CJUE[88]. La procédure d'infraction de la Commission européenne désormais clôturée, cette saga met en lumière les dysfonctionnements graves au sein de l'APD mettant à mal son indépendance et son effectivité. En effet, le 8 novembre 2021, dans un courrier adressé à la Chambre, Alexandra Jaspar, ancienne codirectrice du Centre de connaissance de l'APD et lanceuse d'alerte ayant démissionné en décembre 2021, dénonce le manque d'intégrité de l'ancien président de l'APD, David Stevens, qui dirige le Comité de direction « de manière à en obtenir des décisions

[83] BELGA, « La réforme de l'Autorité de Protection des Données repart pour la quatrième fois au Conseil d'État », 1er juin 2023.
[84] P. LALOUX, « Vie privée : la Belgique une nouvelle fois mise en demeure », disponible sur www.lesoir.be, 6 janvier 2023.
[85] Directive (UE) 2019/1937 du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, *J.O.U.E.*, L305, 26 novembre 2019.
[86] B. DELVAUX et P. LALOUX, « Charlotte Dereppe : « On était à l'APD pour se taire, pas pour protéger la vie privée » », disponible sur www.lesoir.be, 31 octobre 2022.
[87] Loi du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé, *M.B.*, 15 décembre 2022.
[88] P. LALOUX, « De justesse, Frank Robben démissionne de son poste à l'Autorité de protection des données », disponible sur www.lesoir.be, 7 février 2022.

illégales, déloyales et motivées par toute une série de considérations étrangères au souci d'accomplir les missions légales de l'APD »[89]. Elle soutient que « l'APD n'accomplit pas sa tâche générale de contrôle du respect du RGPD et des règles en matière de protection des données en refusant d'agir, de contrôler et de sanctionner certaines institutions, pour ne pas contrarier leurs dirigeants et leurs projets contraires aux règles de droit »[90] et que « l'APD s'efforce de ne pas contrôler ce et ceux qu'elle devrait […] et ne protège pas les données mais ceux qui en font mauvaise usage, pour peu qu'ils soient liés aux autorités publiques »[91]. Il n'y a désormais plus de mandats illégaux à l'APD. La question est à présent de savoir si la réforme de Mathieu Michel sera bénéfique pour la protection des données, ce qui n'est pas certain pour Charlotte Dereppe qui a indiqué dans une interview dans le journal *Le Soir* que « ce qu'on a dénoncé, ce ne sont pas des irrégularités dans la loi. C'est pourtant la loi qu'on change. Ce qu'on a dénoncé, ce sont des pratiques. Ces changements garantissent-ils que les personnes qui sont maintenant en charge de la protection des données vont oser protéger les données et contrôler les autorités publiques ? Quand on voit ce qu'il m'arrive maintenant, c'est tout de même un message très fort à l'égard de ceux qui auraient l'intention de faire de la protection des données sérieusement en ce qui concerne les autorités publiques »[92]. Didier Reynders affirme d'ailleurs que bien qu'il n'existe plus de mandats illégaux au sein de l'APD, les risques de non-indépendance de celle-ci ne sont pas pour autant totalement éradiqués[93].

Une deuxième plainte est déposée en juillet 2020 concernant le Comité de sécurité de l'information (ci-après « CSI ») mis en place après l'adoption du RGPD contre l'avis de la Commission européenne, de l'APD et du Conseil d'État, et dont les décisions sont épinglées pour avoir été prises sans débat parlementaire et sans prise en compte de l'avis de l'APD, et donc de manière illégale[94]. En outre, le CSI ne compte que cinq membres effectifs alors que la loi en prévoit huit[95], membres qui n'ont par ailleurs pas été nommés en bonne et due forme par

[89] P. LALOUX, « Alexandra Jaspar démissionne de l'APD : « le système est toxique » », disponible sur www.lesoir.be, 8 décembre 2021.
[90] P. LALOUX, « Alexandra Jaspar démissionne de l'APD : « le système est toxique » », disponible sur www.lesoir.be, 8 décembre 2021.
[91] P. LALOUX, « Alexandra Jaspar démissionne de l'APD : « le système est toxique » », disponible sur www.lesoir.be, 8 décembre 2021.
[92] B. DELVAUX et P. LALOUX, « Charlotte Dereppe : « On était à l'APD pour se taire, pas pour protéger la vie privée » », disponible sur www.lesoir.be, 31 octobre 2022.
[93] P. LALOUX, « Didier Reynders : « La démission de Frank Robben n'efface pas tous les risques de non-indépendance de l'APD » », disponible sur www.lesoir.be, 8 février 2022.
[94] BELGA, « RGPD : la Commission européenne ouvrira une procédure d'infraction contre la Belgique », disponible sur www.rtbf.be, 9 juin 2021.
[95] Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la

le Parlement[96]. Cette plainte ne fait toutefois pas l'objet d'une procédure en infraction de la part de la Commission européenne[97]. Le rôle du CSI, composé d'une chambre « Sécurité sociale et Santé » et d'une chambre « Autorité fédérale », est de délivrer des autorisations à des institutions ou des organismes publics pour accéder à des données à caractère personnel. Il est le principal outil utilisé par l'exécutif pour autoriser la plupart des traitements de données sensibles pendant la crise de la Covid-19. Par un arrêt du 22 septembre 2022, la Cour constitutionnelle annule l'habilitation faite au CSI d'autoriser la communication de données personnelles à des tiers à des fins de recherche scientifique[98], ce qui a pour effet de priver le Comité de sa raison d'être[99]. Toutefois, le Ministre de la Santé publique, Frank Vandenbroucke, dépose, le 20 décembre 2022, un projet de loi visant à instituer une agence des données de (soins de) santé (ci-après « ADS ») succédant au CSI[100]. Cette agence instituée par une loi du 14 mars 2023[101] prend la forme d'un service administratif à comptabilité autonome au sein du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement[102], et vise à faciliter l'accès et l'échange des données de santé pour le suivi des maladies, la qualité des soins et la recherche[103] de manière sécurisée et transparente[104]. Elle entre en vigueur le 13 avril 2023. La mise en place de l'ADS s'inscrit plus globalement dans le projet de création d'un Espace européen des données de santé. En effet, le 3 mai 2022, la Commission européenne publie un projet de règlement visant à créer un Espace européen des données de santé qui a pour objectif de faciliter une utilisation sécurisée des données à des fins d'utilisation par les particuliers et les professionnels de la santé, de recherche, d'innovation, d'élaboration de politiques et de réglementations. Un projet pilote est mis sur pied, auquel prennent part, notamment, la Belgique, la France, l'Allemagne, la Norvège et la Finlande.

---

protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *M.B.*, 10 septembre 2018, art. 2, §2.

[96] P. LALOUX, « Vie privée : le CSI, gestionnaire de données de santé en (tout) petit comité », disponible sur www.lesoir.be, 5 mai 2021.

[97] P. LAMBERTS, « Protection des données personnelles : la Belgique poursuivie par la Commission ! », disponible sur www.philippelamberts.eu, 9 juin 2021.

[98] C.C., 22 septembre 2022, n°110/2022.

[99] P. LALOUX, « Données de santé : la Cour constitutionnelle détricote le CSI de Frank Robben », disponible sur www.lesoir.be, 22 septembre 2022.

[100] Projet de loi relatif à l'institution et à l'organisation de l'Agence des données de (soins de) santé, *Doc., Ch.*, 2022-2023, n°3065/001.

[101] Loi du 14 mars 2023 relative à l'institution et à l'organisation de l'Agence des données de (soins de) santé, *M.B.*, 3 avril 2023.

[102] Loi du 14 mars 2023 relative à l'institution et à l'organisation de l'Agence des données de (soins de) santé, *M.B.*, 3 avril 2023, art. 2, 2°.

[103] Projet de loi relatif à l'institution et à l'organisation de l'Agence des données de (soins de) santé, exposé des motifs, *Doc., Ch.*, 2022-2023, n°3065/001, p. 4.

[104] Loi du 14 mars 2023 relative à l'institution et à l'organisation de l'Agence des données de (soins de) santé, *M.B.*, 3 avril 2023, art. 4.

Il convient à présent d'étudier la position de l'APD concernant les données de santé, ainsi que ses avancées jurisprudentielles timides en la matière.

La chambre contentieuse est l'organe contentieux administratif de l'APD[105] composée d'un président et de six membres[106]. Elle intervient à la suite d'une plainte déposée par un citoyen ou d'initiative. Elle peut également être saisie par les autorités des États membres européens lorsqu'un dossier concerne un traitement transfrontalier de données[107]. La Chambre contentieuse peut déclarer la plainte recevable, la classer sans suite, ordonner un non-lieu, prononcer la suspension du prononcé ou proposer une transaction[108]. La Chambre contentieuse peut également infliger toute une série de sanctions telles qu'un avertissement ou une réprimande, mais aussi des amendes administratives[109]. Les décisions de l'APD infligeant une amende administrative sont susceptibles d'un recours devant la Cour des marchés dans un délai de trente jours à compter de leur notification[110].

Force est de constater que très peu de décisions de l'APD concernent les données de santé. Il est toutefois à noter que toutes les décisions de l'APD ne font pas l'objet d'une publicité, car cette dernière a le pouvoir de décider au cas par cas de publier ses décisions sur son site internet[111]. Deux affaires méritent en tout cas d'être développées.

La première affaire concerne le manque de transparence dans la déclaration de confidentialité d'une compagnie d'assurance donnant lieu à deux décisions de l'APD. La première décision du 14 mai 2020[112] fait suite au dépôt d'une plainte sur l'utilisation de données de santé obtenues par un assureur hospitalisation (le défendeur) auprès du plaignant à d'autres fins que l'exécution d'obligations découlant de l'assurance hospitalisation sans que le plaignant n'y ait donné son

[105] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 32.
[106] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 34.
[107] Autorité de protection des données, « La Chambre contentieuse dans les grandes lignes », disponible sur www.autoriteprotectiondonnees.be.
[108] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 95,§1.
[109] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 100, §1.
[110] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 108, §2.
[111] Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 95, §1, 8°.
[112] Chambre contentieuse de l'Autorité de protection des données, 14 mai 2020, 24/2020, disponible sur www.autoriteprotectiondonnees.be.

consentement explicite. Le plaignant soutient que pour les autres finalités énumérées dans la déclaration de confidentialité de l'assureur (réalisation de tests informatisés, formation du personnel, prévention des abus et de la fraude, etc.), ainsi que pour le transfert des données à des tiers, l'assureur doit donner le choix à la personne concernée de consentir ou non au traitement de ses données de santé, ce qui n'a pas été le cas en espèce[113]. Le défendeur conteste en arguant qu'il n'est pas nécessaire qu'un consentement distinct soit donné pour chaque transfert de données à caractère personnel, et que pour les traitements énumérés dans la déclaration de confidentialité, le consentement de la personne concernée n'est pas requis, étant donné qu'il ne s'agit pas de données de santé, mais de données « ordinaires », et invoque l'intérêt légitime comme base de licéité de traitement de ces données[114][115]. La Chambre contentieuse considère qu'il y a violation des articles 5, §1, a), 5, §2, 6, §1,12, §1,13, §1,c) et d), et 13, §2 b) du RGPD[116], ordonne au défendeur de se mettre en conformité avec les articles violés, et lui inflige une amende administrative de 50.000 euros[117] pour trois raisons. Premièrement, l'assureur ne précise pas dans sa déclaration de confidentialité le fondement juridique allégué pour chaque finalité de traitement et de transfert des données à caractère personnel. En outre, ce dernier n'opère pas de distinction claire, pour chaque finalité, entre les données à caractère personnel ordinaires et les données de santé, ce qui est pourtant fondamental pour apprécier la pertinence du fondement allégué pour la finalité en cause, d'autant plus que les bases de licéité de traitement des données de santé sont plus restrictives que celles pour le traitement des données ordinaires. Deuxièmement, dans sa déclaration de confidentialité, l'assureur se contente de faire état d'un intérêt légitime sans autre précision pour plusieurs des finalités énumérées dans sa déclaration, ce qui est contraire à l'obligation d'information imposée au responsable du traitement par l'article 13, §1, d) du RGPD. Troisièmement, la déclaration de confidentialité ne mentionne pas la possibilité pour la personne concernée d'exercer son droit d'opposition garanti à l'article 21, §2 du RGPD[118]. Cette décision fait l'objet d'un réexamen par la Chambre contentieuse à la suite d'un arrêt de

[113] Chambre contentieuse de l'Autorité de protection des données, 14 mai 2020, 24/2020, disponible sur www.autoriteprotectiondonnees.be, p. 2.
[114] Chambre contentieuse de l'Autorité de protection des données, 14 mai 2020, 24/2020, disponible sur www.autoriteprotectiondonnees.be, p. 3
[115] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 6, §1, f).
[116] Chambre contentieuse de l'Autorité de protection des données, 14 mai 2020, 24/2020, disponible sur www.autoriteprotectiondonnees.be, p. 13.
[117] Chambre contentieuse de l'Autorité de protection des données, 14 mai 2020, 24/2020, disponible sur www.autoriteprotectiondonnees.be, p. 16 et 17.
[118] J.-M. BINON, *op. cit.*, p. 1958.

la Cour des marchés du 18 novembre 2020 qui annule la décision du 14 mai 2020 au motif que le défendeur doit avoir la possibilité, une fois les griefs formulés clairement par écrit, de remettre des conclusions écrites à ce sujet[119]. Par une décision du 6 mai 2021, la Chambre contentieuse considère que bien que des modifications aient été apportées à la déclaration de confidentialité de l'assureur pour se mettre en conformité avec le RGPD, ce qui constitue un élément favorable dans la détermination du montant de l'amende administrative, ces dernières ne sont pas de nature annuler rétroactivement les violations constatées[120]. Par conséquent, elle décide de ramener le montant de l'amende administrative à 30.000€[121].

La dernière décision de l'APD qui concerne les données de santé est une décision du 19 juillet 2022[122]. La Chambre contentieuse est saisie à la suite d'une plainte déposée par une employée à l'encontre de son supérieur hiérarchique dans laquelle elle dénonce la communication de données à caractère personnel relatives à sa santé (le départ de la plaignante pour cause d'inaptitude au travail) lors d'une réunion de service à laquelle elle ne participe pas, consignées dans le procès-verbal de réunion[123]. La plaignante ne conteste pas la licéité du traitement de ses données de santé dans sa finalité première (recevoir l'information et la traiter au niveau des services des ressources humaines à des fins du personnel), mais la communication ultérieure de ses données de santé à l'ensemble du personnel de la défenderesse pour les informer sur les mouvements du personnel[124]. La Chambre contentieuse rappelle que « le traitement de données à caractère personnel opéré pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement ne peut être autorisé conformément à l'article 5, §1, b) du RGPD que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement »[125]. En l'espèce, la Chambre contentieuse conclut que cette communication n'est pas compatible avec la finalité initiale, de sorte qu'une

[119] Chambre contentieuse de l'Autorité de protection des données, 14 mai 2020, 24/2020, disponible sur www.autoriteprotectiondonnees.be, p. 5.
[120] Chambre contentieuse de l'Autorité de protection des données, 6 mai 2021, 57/202, disponible sur www.autoriteprotectiondonnees.be, p. 34.
[121] Chambre contentieuse de l'Autorité de protection des données, 6 mai 2021, 57/202, disponible sur www.autoriteprotectiondonnees.be, p. 35.
[122] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be.
[123] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be, p. 2.
[124] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be, p. 8.
[125] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be, p. 8 et 9.

base licéité de traitement distincte est requise pour que cette communication soit licite[126], ce dont la défenderesse ne fait pas état. Par ailleurs, la Chambre contentieuse est d'avis que la communication en l'espèce ne peut se fonder sur aucune base de licéité propre[127]. Elle considère donc que la défenderesse a violé les articles 5, §1, b) juncto, 6, §4 et 9, §2 lus en combinaison avec l'article 6, §1 du RGPD[128], et condamne la défenderesse à une réprimande et à « prendre les mesures nécessaires pour restreindre, voire supprimer […] la diffusion des informations relatives à la santé de la plaignante »[129] .

Au sein de ce Paragraphe, nous avons souhaité revenir sur le contexte d'entrée en vigueur du RGPD, ainsi que sur les particularités de cette nouvelle législation européenne. D'application directe, elle a des impacts certains sur le développement du droit belge en la matière. Cet impact est par ailleurs illustré par le renforcement du rôle des autorités de contrôle nationales. Cependant, et c'est ce que nous avons démontré, une telle autorité de contrôle doit son bon fonctionnement à son indépendance – caractéristique qui a été plusieurs fois déclarée manquante concernant l'APD belge, portant une atteinte certaine à sa réputation auprès du grand public. Par ailleurs, l'APD ne se caractérise pas par une jurisprudence abondante au regard des données des santé et des assurances, au contraire de son homologue français. À ce stade, il est difficile d'avoir une explication nette, mais nous pouvons poser l'hypothèse que cela est lié à son institution relativement récente tandis que la CNIL, l'autorité de contrôle française, existe depuis 1978. En ce sens, pour le droit belge, il est tout aussi important de se tourner vers la jurisprudence des autres juridictions nationales.

La Section première revient sur l'histoire de la protection des données à caractère personnel en Belgique. Il est certain qu'il s'agit d'une protection marquée de façon croissante par le droit de l'Union européenne, et c'est pour cette raison qu'il nous a semblé nécessaire de revenir sur les évolutions de ce droit. Au regard de ces propos génériques nous présentant une harmonisation attendue, il est utile, désormais, d'étudier de façon précise le régime juridique des assurances en lien avec la protection des données de santé, ce qui fera l'objet de notre Section 2.

---

[126] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be, p. 9.
[127] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be, p. 10.
[128] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be, p. 11.
[129] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be, p. 12.

## Section 2. L'articulation ambiguë entre le droit des assurances et le nouveau régime de traitement des données de santé

Au sein de cette Section, nous allons analyser les modalités selon lesquelles les assurances se sont affirmées comme les protectrices légitimes des données de santé (**§1**) avant d'étudier les limites de cet aspect collaboratif qui transparaissent à travers l'étude des bases de licéité du traitement des données de santé (§**2**).

### §1. Des assurances s'affirmant comme les protectrices légitimes des données de santé : un aspect collaboratif

Au sein de ce Paragraphe, nous donnerons quelques précisions sur les assurances concernées par le traitement des données de santé et nous mettrons en avant la collaboration des assurances avec les autorités de protection des données.

Le RGPD impacte particulièrement les assurances, étant donné que les données, dont les données de santé, sont au cœur de leurs activités. Cela est d'autant plus marquant que le monde des assurances est en pleine transformation digitale (souscription de contrat en ligne, actes de gestion en ligne, etc.), ce qui a pour conséquence que le volume de données à caractère personnel traitées est de plus en plus important[130].

Le droit des assurances entretient donc des liens étroits et complexes avec la protection des données à caractère personnel concernant la santé et le respect de la vie privée. En effet, au stade de la souscription du contrat d'assurance, il est important pour l'assureur de collecter des informations relatives à l'état de santé du candidat afin d'apprécier le risque à assurer, et le cas échéant, de calculer de manière adéquate la prime dans le cas où il accepte de couvrir le risque. En outre, lorsqu'un sinistre survient, l'assureur a également besoin d'obtenir des informations relatives à la santé de l'assuré afin de déterminer, en fonction des circonstances de survenance du sinistre, si la prestation convenue dans le contrat lui est due, et d'évaluer correctement le dommage à indemniser[131]. L'évaluation des risques et des dommages par les assureurs a ainsi pour corollaire nécessaire un droit d'information aboutissant au principe de la déclaration

[130] N. BENHATTA et H. CHAMBA, *Appliquer le RGPD dans l'assurance*, 2e éd., Paris, L'Argus de l'assurance Éditions, 2022, p. 16 à 18.
[131] Assuralia, « La protection de vos données de santé chez l'assureur », disponible sur www.abcassurance.be.

spontanée du risque par le candidat-preneur d'assurance selon lequel le candidat à l'assurance a, en principe, l'obligation de déclarer à l'assureur toute circonstance pertinente connue de lui[132]. Les assurances qui sont amenées à collecter des données de santé sont principalement les assurances de personnes. Une assurance de personnes peut être définie comme « l'assurance dans laquelle la prestation d'assurance ou la prime dépend d'un évènement incertain qui affecte la vie, l'intégrité physique ou la situation familiale d'une personne »[133] (l'assurance maladie, soins de santé, vie, solde restant dû, etc.). Les assurances de dommages sont également parfois amenées à collecter des données de santé, notamment certaines assurances de responsabilité. Nous pensons, par exemple, à l'assurance R.C. auto qui collecte des données de santé pour évaluer le dommage d'un tiers victime d'un accident de la route causé par son assuré ou à une assurance voyage en cas d'annulation pour cause de maladie.

Ainsi, nous pouvons voir que les acteurs de l'assurance interviennent en tant que responsable de traitement, de sous-traitant ou de responsable de traitement conjoint au sens du RGPD[134]. Le RGPD définit le responsable de traitement comme « la personne physique ou morale, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens de traitement »[135]. La notion de responsable de traitement est une notion autonome et propre à la réglementation en matière de protection des données qu'il convient d'apprécier eu égard aux critères qu'elle énonce : « la détermination des finalités du traitement de données concerné ainsi que celles des moyens de celui-ci »[136]. Bien que le Comité européen de la protection des données affirme qu'une personne physique puisse être considérée comme responsable de traitement, dans la pratique, c'est généralement l'organisation au sein de laquelle la personne physique travaille qui sera considérée comme responsable du traitement au sens du RGPD[137]. Il convient toutefois de préciser qu'il y a toujours lieu de procéder à une analyse au cas par cas pour qualifier une personne de responsable de traitement, et qu'il existe un flou

[132] Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, art. 58.
[133] Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, art. 5, 16°.
[134] CNIL, « La qualification des acteurs du secteur de l'assurance au regard du RGPD », disponible sur www.cnil.fr, 16 juillet 2021.
[135] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 4, 7).
[136] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be, p. 7.
[137] Comité européen de la protection des données, « Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD », disponible sur www.edpb.europa.eu, 7 juillet 2021, p. 3.

autour de cette notion pouvant donner lieu à des doutes sur la qualification à donner[138]. En effet, l'APD souligne, à plusieurs reprises, qu'il s'agit d'une notion difficilement cernable par une personne ne maîtrisant pas la matière, de sorte qu'il est souvent complexe pour le plaignant d'identifier correctement le responsable du traitement à l'égard duquel il porte plainte[139]. Il est par ailleurs intéressant de noter que la CJUE interprète de manière extensive la notion de responsable de traitement, de sorte, par exemple, à y introduire une communauté religieuse conjointement avec ses membres prédicateurs[140]. Nous pouvons en tout cas affirmer qu'un assureur est considéré comme responsable de traitement au sens du RGPD pour les traitements relatifs à l'exécution d'un contrat d'assurance[141].

La manière dont les assurances appréhendent le nouveau droit lié à la protection des données à caractère personnel est surtout visible depuis l'entrée en vigueur du RGPD, et résulte de cette politique d'harmonisation des droits nationaux. En effet, partout dans l'Union européenne, les assurances sont invitées à se conformer aux nouvelles dispositions de la protection des données qui offrent un régime de protection accru à plusieurs égards. Il semble que les compagnies d'assurance embrassent ce rôle et collaborent activement avec les autorités de protection des données nationales afin de s'afficher comme des alliées de taille dans la protection des données[142]. Par ailleurs, la logique de dialogue entre la Commission européenne, les autorités de protection de données nationales et les assurances est également mise en avant par le Comité européen des assurances qui travaille avec diligence comme intermédiaire entre les assurances nationales et les acteurs européens[143].

Cette collaboration est la suite logique de l'esprit du RGPD. En effet, celui-ci est marqué par une volonté générale de responsabiliser les acteurs intervenant dans le processus de traitement des données à caractère personnel, en privilégiant notamment un système où les acteurs doivent prouver leur conformité aux dispositions du RGPD plutôt que de remplir des formalités

---

[138] N. BENHATTA et H. CHAMBA, *op. cit.*, p. 28.
[139] Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be ; Chambre contentieuse de l'Autorité de protection des données, 9 juillet 2021, 76/2021, disponible sur www.autoriteprotectiondonnees.be ; Chambre contentieuse de l'Autorité de protection des données, 23 décembre 2020, 81/2020, disponible sur www.autoriteprotectiondonnees.be.
[140] C.J., arrêt *Land Hessen*, 9 juillet 2020, C-272/19, EU:C:2020:535 ; C.J., arrêt *Fashion ID*, 29 juillet 2019, C-40/17, EU:C:2019:629 ; C.J., arrêt *Jehovan todistajat*, 10 juillet 2018, C-25/17, EU:C:2018:551 ; C.J., arrêt *Wirtschaftsakademie Schleswig Holstein*, 5 juin 2018, C-210/16, EU:C:2018:388.
[141] N. BENHATTA et H. CHAMBA, *op. cit.*, p. 28.
[142] N. BENHATTA et H. CHAMBA, *ibidem*, p. 64 et *s*.
[143] Insurance Europe, « Insurers highlight challenges of applying GDPR », disponible sur www.insuranceeurope.eu, 11 avril 2019.

préalables. Ainsi, il appartient aux assurances en tant que responsables de traitement et aux sous-traitants d'être en mesure de démontrer cette conformité[144]. En effet, conformément à l'article 24, §1 du RGPD, « compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques dont le degré de portabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaires ». Ce principe est analysé, par Nordine Benhatta et Hugues Chamba, comme étant celui d'*accountability* ou de responsabilité découlant par ailleurs des considérants 74 (« le responsable de traitement doit être à même de démontrer la conformité des activités de traitement au règlement RGPD ») et 85 (« dès que le responsable du traitement apprend qu'une violation des données à caractère personnel s'est produite, il convient qu'il le notifie à l'autorité de contrôle dans les meilleurs délais et, lorsque c'est possible, 72 heures au plus tard après avoir pris connaissance, à moins qu'il ne puisse démontrer, conformément au principe de responsabilité, qu'il est peu probable que la violation en question engendre un risque pour les droits et libertés des personnes physiques »)[145].

Dans le cadre de cette étude, nous avons pu identifier deux manifestations différentes de la collaboration des assurances, comme corollaire du principe de responsabilité. En effet, il est possible de distinguer une collaboration par respect des obligations énoncées au sein RGPD, par la prise de connaissance de ces obligations légales et par leur application. Mais il apparaît que les assurances tendent également à adopter une approche proactive, et préventive de diffusion de l'information. Nous pouvons revenir sur ces aspects.

Le RGPD prévoit en effet plusieurs obligations pour les responsables de traitement. Ainsi, au fondement de l'article 30, il est attendu des assurances qu'elles tiennent des registres de traitement[146]. Par ailleurs, elles sont invitées à procéder à des analyses d'impact relatives à la protection des données pour les traitements susceptibles d'engendrer des risques élevés pour

[144] N. BENHATTA et H. CHAMBA, *op. cit.*, p. 11 ; T. DAUTIEU, « La commission nationale de l'informatique et des libertés, régulateur des données de santé », *Les tribunes de la santé*, vol. 1, n°58, 2018, p. 51 et 52.
[145] N. BENHATTA et H. CHAMBA, *ibidem*, p. 102.
[146] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 30.

les droits et libertés des personnes, au fondement des articles 35 et 36[147]. Elles sont également tenues d'encadrer tout transfert de données en-dehors de l'Union européenne selon les articles 44 à 50[148]. Enfin, les assurances sont tenues de documenter toutes les violations des données et de renseigner les mesures prises pour remédier à ces violations, au fondement des articles 33 et 34[149]. En plus de cela, les assurances se doivent d'informer les preneurs d'assurance de leurs droits, sauvegarder les recueils de consentement et mettre en place des procédures d'exercice de droits[150].

Par ailleurs, dans la logique du principe d'*accountability*, les assurances sont aussi tenues de nommer un délégué de protection de données (DPD) ou data protection officer (DPO), au fondement de l'article 37, §1, b) et c), dès lors que « les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ou les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 »[151]. Toujours selon Nordine Benhatta et Hugues Chamba, « s'agissant des acteurs du marché de l'assurance et plus particulièrement des organismes assureurs et des courtiers de taille significative dont le volume de données est important, la présence de données sensibles est courante et la complexité des traitements est avérée, le niveau de compétence du DPO devra être élevé »[152].

Il est attendu, depuis l'entrée en vigueur du RGPD, que les assurances se conforment activement aux dispositions du Règlement concerné. Pour ce faire, des diagnostics de conformité sont menés au sein des pays de l'Union européenne, conduisant à la rédaction de packs de

[147] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 35 et 36.
[148] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 44 à 50.
[149] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 33 et 34.
[150] N. BENHATTA et H. CHAMBA, *ibidem*, p. 102 à 108 ; Commission nationale pour la protection des données du Grand-Duché de Luxembourg, « Documentation et responsabilisation », disponible sur www.cdnp.public.lu, 19 juin 2018.
[151] N. BENHATTA et H. CHAMBA, *ibidem*, p. 133 et 134.
[152] N. BENHATTA et H. CHAMBA, *ibidem*, p. 135 à 141.

conformité. En ce sens, en France, la CNIL consacre plusieurs fiches (6) explicatives afin d'assister les assurances dans la conformité avec le RGPD, ainsi qu'avec la législation française[153]. En effet, « le secteur de l'assurance bénéficie depuis de nombreuses années d'un accompagnement spécifique de la CNIL compte tenu des enjeux liés aux traitements mis en œuvre, notamment en ce qu'ils impliquent souvent des données de santé. Dans ce cadre, la CNIL anime régulièrement des « clubs conformité » avec les principaux représentants du secteur (France assureurs, le Centre technique des institutions de prévoyance, la Fédération nationale de la mutualité française) »[154].

Suivant cette logique, est rédigé en juillet 2021, en association avec la CNIL, un guide actualisant les principes inscrits dans le pack de conformité de la CNIL[155]. Il est intéressant de noter que le point 6 accorde une place importante et particulière au traitement des données de santé, rappelant qu'il s'agit de données bénéficiant d'une protection accrue et autrement protégées par des législations nationales spécifiques[156]. En Belgique, Assuralia, l'Union professionnelles des entreprises d'assurances belges, ne présente pas d'équivalents de ces packs de conformité. Cependant, elle affiche des efforts dans la diffusion de l'information concernant les dispositions du RGPD de façon sectorielle, *i.e.* selon le champ d'exercice des assurances. Ainsi, par exemple, Assuralia consacre une brochure à la question de la « Protection de vos données de santé chez l'assureur », publiée en 2021, qui revient sur les droits des preneurs d'assurance et en particulier sur l'impact du RGPD sur de tels droits[157].

---

[153] CNIL, « Les grands traitements du secteur de l'assurance et leurs bases légales », disponible sur www.cnil.fr, 16 juillet 2021 ; CNIL, « Adopter les six bons réflexes », disponible sur www.cnil.fr, 18 septembre 2019 ; CNIL, « La qualification des acteurs du secteur de l'assurance au regard du RGPD », disponible sur www.cnil.fr, 16 juillet 2021 ; CNIL, « Les durées de conservation des données du secteur de l'assurance », disponible sur www.cnil.fr, 16 juillet 2021 ; CNIL, « Le principe de minimisation et les traitements du NIR et des données de santé dans le secteur de l'assurance », disponible sur www.cnil.fr, 16 juillet 2021 ; CNIL, « Droit des personnes et profilage : les spécificités du secteur de l'assurance », disponible sur www.cnil.fr, 16 juillet 2021 ; France assureurs, « Traitement des données à caractère personnel : guide d'actualisation du Pack de conformité assurance », disponible sur www.franceassureurs.fr, 15 juillet 2021 ; CNIL, « Les fiches pratiques pour le secteur de l'assurance », disponible www.cnil.fr.

[154] CNIL, « Rapport annuel 2021 », disponible sur www.cnil.fr, p. 36 : 25% des requêtes traitées par la CNIL concernent le secteur de la banque, celui du crédit et celui des assurances ; C. BONNIER, « La CNIL surveille le secteur de l'assurance », disponible sur www.actu-juridique.fr, 12 mai 2022.

[155] France assureurs, « Guide actualisant le Pack de conformité Assurance », disponible sur www.franceassureurs.fr.

[156] France assureurs, « Guide actualisant le Pack de conformité Assurance », disponible sur www.franceassureurs.fr, p. 36 et 37.

[157] Assuralia, « La protection de vos données de santé chez l'assureur », disponible sur www.abcassurance.be, 2021.

Par ailleurs, en plus de publiciser les droits des preneurs d'assurance en vertu du RGPD, les assurances et les courtiers n'hésitent pas à sensibiliser ou former le personnel aux nouvelles dispositions du Règlement. Ainsi, se multiplient les « séminaires, sessions d'informations, workshops et colloques organisés sur le thème du RGPD »[158].

Ce Paragraphe a eu pour enjeu d'étudier le rôle des assurances dans la protection des données à caractère personnel et notamment dans la protection des données sensibles. Cela a nécessité de revenir brièvement sur la notion même de responsable de traitement. Il semble, à partir de cette étude, que les assurances ont mobilisé divers outils afin de se conformer aux nouvelles dispositions du RGPD, découlant du principe d'*accountability.* Si un tel principe est séduisant, de prime abord, il fait peser sur les responsables de traitement la charge de démontrer leur conformité aux dispositions du RGPD, retirant ce droit aux autorités de protection de données. Par ailleurs, si les assurances et les sous-traitants s'activent dans la protection des données à caractère personnel, ces responsables de traitement n'en restent pas moins une source de violation importante de cette protection, ce qui constituera le cœur du Paragraphe 2.

## §2. La problématique des bases de licéité de traitement des données de santé dans le secteur des assurances

Comme nous l'avons vu, l'article 9, §2 du RGPD prévoit un certain nombre de dérogations au principe d'interdiction de traitement des données de santé. La seule base juridique sur laquelle peuvent se fonder les assureurs pour traiter des données de santé est le consentement explicite de la personne concernée[159]. Toutefois, cette base de licéité de traitement pose un certain nombre de problèmes en pratique, tant pour les assureurs que pour les candidats à l'assurance – les assurés. Dans le présent paragraphe, il sera question d'examiner si le consentement explicite de la personne concernée constitue une base de traitement appropriée. Par ailleurs, le RGPD laisse aux États membres la possibilité de prévoir des bases de traitement supplémentaires dans leur ordre juridique national[160], possibilité dont se sont saisis plusieurs États membres qui ont introduit une base juridique de traitement des données de santé qui ne

[158] Assurdeal, « Les courtiers belges ont aussi à se mettre en conformité #GDPR (#RGPD en France) », disponible sur www.assurdeal.media, 9 mai 2018.
[159] J. AMANKWAH, « In het licht van de AVG : het verwerken van bijzondere categorieën van persoonsgegevens in de verzekeringssector », *T.B.H.*, 2019/2, p. 245.
[160] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 9, §4.

dépend pas du consentement explicite de la personne concernée[161]. Dès lors, il sera également question d'examiner si l'introduction d'une base juridique de traitement autre que le consentement explicite de la personne concernée constitue une solution appropriée pour le secteur des assurances.

L'article 9, §2, a) du RGPD prévoit que des données de santé peuvent être traitées si « la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ». En plus d'être explicite, le consentement doit répondre aux exigences de l'article 4, 11) du RGPD, à savoir qu'il doit être libre, spécifique, éclairé et univoque[162]. Selon le considérant 42 du RGPD, « le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice ». Il est également à noter que cette dérogation n'est pas valable lorsque la personne concernée est dans une situation de dépendance vis-à-vis du responsable de traitement, ayant pour effet de l'empêcher de refuser librement son consentement[163].

Ainsi, nous pouvons nous interroger quant au caractère réellement libre du consentement du candidat à l'assurance – ou de l'assuré - donné à l'assureur pour traiter ses données de santé lorsqu'on sait que le refus du candidat – ou de l'assuré – à donner son consentement exposerait ce dernier soit à un refus de l'assureur de conclure le contrat ou d'intervenir, soit à l'application d'une surprime[164]. À titre d'exemples, on retrouve sur le site d'Ethias la mention suivante : « Ce consentement peut être retiré à tout moment mais cela n'invalidera en rien les traitements de données déjà effectués. Par ailleurs, dans ce cas, Ethias pourrait se retrouver dans l'impossibilité de donner suite à vos demandes de conclusion d'un contrat d'assurance ou d'indemnisation de sinistre(s) »[165], et dans la déclaration de confidentialité d'Allianz la mention suivante : « À défaut de consentir au traitement de données relatives à la santé, nous serons dans l'impossibilité de gérer votre police d'assurance si une garantie corporelle devait avoir été

[161] J.-M. BINON, *op. cit*., p. 1962.
[162] J.-M. VAN GYSEGHEM, *op. cit*., p. 272.
[163] J.-M. VAN GYSEGHEM, *ibidem*, p. 272.
[164] J.-M. BINON, *op. cit*., p. 1961.
[165] Ethias, « Traitement de données relatives à la santé et/ou autres donnés sensibles », disponible sur www.ethias.be.

souscrite ou si un sinistre avec dommage à la santé survenait »[166]. Il est dès lors légitime de se demander si le candidat à l'assurance – ou l'assuré – ne se retrouve pas dans une situation de dépendance ou de faiblesse telle vis-à-vis de l'assureur que son consentement au traitement de ses données de santé ne revêt pas un caractère libre.

Le 16 juin 2003, le Tribunal de commerce de Bruxelles conclut que le consentement revêt un caractère libre s'agissant d'une assurance hospitalisation eu égard au caractère facultatif de cette assurance et à la possibilité du candidat à l'assurance de consentir ou non au traitement de ses données de santé[167]. Il convient toutefois de noter qu'il s'agit d'une décision rendue sous l'empire du droit antérieur au RGPD.

La question du caractère libre du consentement se pose davantage dans le cadre de l'assurance solde restant dû, car bien que non obligatoire légalement, l'accès au crédit hypothécaire et donc à la propriété est conditionné à la souscription d'une telle assurance et donc à l'acceptation, par le candidat à l'assurance, du traitement de ses données de santé[168]. En effet, il ressort d'un entretien avec un médecin généraliste qu'à la souscription d'une assurance solde restant dû, les assureurs sont particulièrement vigilants quant à la consommation d'alcool et de tabac du candidat à l'assurance, ainsi qu'à l'existence de cancers et de maladies psychiatriques dont ce dernier pourrait être atteint. Toutefois, dans trois jugements du 9 mars 2018, le président du Tribunal de commerce francophone de Bruxelles considère que le candidat à l'assurance solde restant dû ne se trouve pas dans une situation de dépendance ou d'infériorité vis-à-vis de l'assureur comparable à celle qui existe entre un employé et son employeur, potentiel ou actuel, car le traitement des données de santé auquel il consent lors de la souscription du contrat d'assurance vise à lui procurer un avantage, à savoir la couverture du risque de décès en cours de remboursement du prêt hypothécaire par l'assureur[169]. Selon Jean-Marc Binon, il est permis de douter de la compatibilité de cette interprétation particulièrement large du caractère libre du consentement avec l'article 4, 11) et le considérant 42 du RGPD, ainsi qu'avec les lignes directrices sur le consentement du Groupe de travail « Article 29 »[170], desquels il est possible

[166] Allianz, « Déclaration sur la protection des données personnelles », disponible sur www.allianz.be, novembre 2021, p. 7.
[167] Comm. Bruxelles (cess.), 16 juin 2003, *Test-Achats/DKV Belgium*, *R.D.C.*, 2003, p. 901.
[168] J.-M. BINON, *op. cit.*, p. 1961.
[169] Comm. Bruxelles (cess.), 9 mars 2018, A/17/01046 ; Comm. Bruxelles (cess.), 9 mars 2018, A/17/01140 ; Comm. Bruxelles (cess.), 9 mars 2018, A/17/01141.
[170] Groupe de travail « article 29 », « Lignes directrices sur le consentement au sens du règlement 2016/679 », disponible sur www.cnil.fr, 10 avril 2018.

de déduire l'existence d'un rapport de force entre l'assureur et le candidat à l'assurance solde restant dû comparable à celui qui existe entre un employeur et un candidat à l'emploi[171]. Il est à préciser qu'Insurance Europe s'est posé la question de savoir si le consentement revêt un caractère libre dans le secteur des assurances[172]. Le Groupe de travail « Article 29 » n'a toutefois pas abordé cette question dans les lignes directrices précitées.

Outre la problématique du caractère libre du consentement, cette base de traitement du consentement explicite pose, selon les représentants des entreprises d'assurance et des intermédiaires d'assurance, de nombreuses difficultés en pratique. En effet, selon ces derniers, cette base de traitement serait appliquée de manière très variée dans le secteur des assurances, et augmenterait considérablement leur charge administrative[173]. En outre, le consentement est précaire, en ce sens que l'article 7, §3 du RGPD confère à la personne concernée le droit de retirer son consentement, ce qui peut avoir comme conséquence de rendre la conclusion du contrat ou la gestion du sinistre plus compliquée voire entravée, et de créer des difficultés quant à la preuve d'une fraude ou d'une omission volontaire. Ils regrettent également l'absence de précision dans le RGPD sur la durée de validité du consentement donné et sur son renouvellement périodique[174]. Par ailleurs, dans le cadre des assurances de personnes pour compte, il serait particulièrement difficile d'obtenir et de prouver ce consentement[175]. Compte tenu des problèmes que soulève cette base de traitement, les représentants des entreprises d'assurance et des intermédiaires d'assurance souhaiteraient que la loi du 30 juillet 2018 relative à la vie privée prévoie une base de traitement alternative des données de santé dans le secteur des assurances[176].

Après avoir constaté que le Royaume-Uni, l'Irlande, les Pays-Bas et l'Espagne se fondent sur l'article 9, §2, g), h) et/ou i) du RGPD pour introduire une base de traitement des données de santé dans le secteur des assurances qui ne dépende pas du consentement explicite de la

[171] J.-M. BINON, *op. cit*., p. 1961.
[172] Insurance Europe, « Insurance Europe comments on consent », disponible sur www.insuranceeurope.eu, 17 juin 2017.
[173] Avis de la Commission des assurances concernant le traitement des données relatives à la santé dans le cadre du règlement UE 2016/679 (règlement général sur la protection des données), Doc/C2019/1, 16 juillet 2019, p. 3.
[174] Avis de la Commission des assurances concernant le traitement des données relatives à la santé dans le cadre du règlement UE 2016/679 (règlement général sur la protection des données), Doc/C2019/1, 16 juillet 2019, p. 4.
[175] Avis de la Commission des assurances concernant le traitement des données relatives à la santé dans le cadre du règlement UE 2016/679 (règlement général sur la protection des données), Doc/C2019/1, 16 juillet 2019, p. 3.
[176] Avis de la Commission des assurances concernant le traitement des données relatives à la santé dans le cadre du règlement UE 2016/679 (règlement général sur la protection des données), Doc/C2019/1, 16 juillet 2019, p. 4.

personne concernée[177], la Commission des assurances propose d'insérer dans la loi du 30 juillet 2018 les articles 8, §1bis et §1ter « qui, prenant appui sur l'article 9, 2., sous h), du RGPD à l'instar de la solution retenue, notamment aux Pays-Bas, entendraient permettre aux assureurs, réassureurs et aux intermédiaires d'assurance de traiter de données de santé « strictement nécessaires » à une série de finalités identifiées de manière exhaustive, à moins d'une objection de la personne concernée qui équivaudrait à un retrait de consentement au sens de l'article 7, 3., du RGPD »[178]. L'APD, dans sa décision n°24/2020, invite aussi le législateur à prévoir une base de traitement des données de santé dans le secteur des assurances « qui permette la collecte de données de santé dans des limites bien définies dans le cadre de la relation (pré)contractuelle entre l'assureur et l'assuré »[179]. Il est à noter que lors de l'élaboration de la loi du 30 juillet 2018, un amendement est déposé en vue d'introduire une base de traitement spécifique aux assurances sur la base de l'article 9, §2, h) du RGPD. Cet amendement est retiré à la suite de la remarque du secrétaire d'État selon laquelle il vaut mieux éviter de réglementer des situations spécifiques dans une loi-cadre[180].

C'est dans ce contexte qu'une note de politique générale en matière d'économie est prise le 4 novembre 2020, indiquant l'adoption de dispositions légales afin que soit autorisé le traitement des données de santé par les compagnies d'assurance dans le cadre de certaines finalités, et ce dans le respect du RGPD[181]. À la suite de cette note, Pierre-Yves Dermagne, vice-premier Ministre et Ministre de l'Économie et du Travail, rédige un avant-projet de loi relatif au traitement des données à caractère personnel concernant la santé. L'exposé des motifs de l'avant-projet de loi indique que la législation belge ne contenant aucune disposition spécifique pour le traitement des données de santé dans le cadre des assurances, le traitement de celles-ci est conditionné et n'est possible que par le consentement explicite et préalable de la personne concernée sur la base de l'article 9, §2, a) du RGPD. Le consentement explicite et préalable n'étant pas considéré comme une base juridique fiable et qui ralentit, par ailleurs, souvent le processus d'indemnisation, l'avant-projet de loi prévoit l'introduction d'une base de traitement

[177] Avis de la Commission des assurances concernant le traitement des données relatives à la santé dans le cadre du règlement UE 2016/679 (règlement général sur la protection des données), Doc/C2019/1, 16 juillet 2019, p. 6 à 8.
[178] J.-M. BINON, *op. cit.*, p. 1963.
[179] Chambre contentieuse de l'Autorité de protection des données, 14 mai 2020, 24/2020, disponible sur www.autoriteprotectiondonnees.be, p. 16.
[180] Avis de la Commission des assurances concernant le traitement des données relatives à la santé dans le cadre du règlement UE 2016/679 (règlement général sur la protection des données), Doc/C2019/1, 16 juillet 2019, p. 2.
[181] Avis de la Commission des assurances sur l'avant-projet de loi relatif au traitement des données à caractère personnel concernant la santé, Doc/C2021/3, 20 décembre 2021, p. 1.

de ces données alternative, à savoir le traitement de ces dernières pour des motifs d'intérêt public important, en s'appuyant sur les articles 6, §1, e) et 9, §2, g) du RGPD. L'avant-projet prévoit dès lors l'introduction, dans la quatrième partie, titre II, chapitre 1er de la loi du 4 avril 2014 relatives aux assurances, une section Iter intitulée « Données à caractère personnel concernant la santé » comportant un nouvel article 61/5, §§1-8[182].

Le 20 décembre 2021, la Commission des assurances est amenée à rendre un avis sur cet avant-projet de loi à la suite d'une demande d'avis formulée le 13 septembre 2021 par Pierre-Yves Demargne[183]. L'avis formulé par la Commission des assurances nous aide à prendre connaissance des arguments de trois types d'acteurs, permettant ainsi d'englober les enjeux liés à l'avant-projet de loi concerné : il s'agit de la délégation des consommateurs, de la délégation des assurances, et des experts. Il est à noter que ces délégations ne sont pas unanimes quant à la nécessité d'introduire une base de traitement de ces données par les entreprises d'assurance autre que le consentement explicite et préalable de la personne concernée. Il importe donc d'exposer les différents arguments.

Les représentants des consommateurs souhaitent le maintien, comme unique base de traitement des données de santé par les entreprises d'assurance et de réassurance, le consentement explicite et préalable tel que fixé à l'article 9, §2, a) du RGPD. Ces derniers contestent l'argument selon lequel le consentement explicite et préalable ne constituerait pas une base juridique fiable et qui ralentirait le processus d'indemnisation. Ils estiment que la dérogation à cette exigence conduirait à un affaiblissement important de la protection des données et du droit au respect de la vie privée. Ce faisant, ces représentants tiennent à rappeler la nature juridique particulière des données de santé qui méritent une protection accrue. Cela est attesté par le régime juridique existant, tant au niveau national qu'au niveau régional et européen. Par ailleurs, l'argument des délégations représentant les entreprises d'assurance est fortement affaibli en ce que le RGPD cite explicitement le cas des « compagnies d'assurance »[184] comme des tiers qui ne peuvent être impliqués dans le traitement des données « concernant la santé pour des motifs d'intérêt

[182] Avis de la Commission des assurances sur l'avant-projet de loi relatif au traitement des données à caractère personnel concernant la santé, Doc/C2021/3, 20 décembre 2021, p. 2.
[183] Avis de la Commission des assurances sur l'avant-projet de loi relatif au traitement des données à caractère personnel concernant la santé, Doc/C2021/3, 20 décembre 2021, p. 1.
[184] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L 119/1, 4 mai 2016, considérant n°52.

public »[185]. Enfin, le traitement « nécessaire pour des motifs d'intérêt public important »[186] relève des prérogatives des missions d'ordre public et non pas celles des entreprises d'assurance[187].

Les représentants des entreprises d'assurance soutiennent quant à eux cette initiative et renvoient aux problèmes que soulève le consentement explicite et préalable comme base de traitement des données de santé dans la pratique, ainsi que dans la législation des autres États membres. Ils rappellent que le droit au respect de la vie privée (article 8 de la CEDH) n'est pas un droit absolu, mais qu'il est soumis à certaines conditions, conditions que l'avant-projet de loi satisfait selon eux. En outre, ils estiment que les activités des entreprises d'assurance relèvent de la notion d'« intérêt public » et renvoient à cet égard à l'article 1:12, 4° du Code des sociétés et des associations. Cet argument est contesté par les représentants des consommateurs estimant que la notion d' « intérêt public » est ajoutée afin d'accroître la confiance du public. Les représentants des assureurs soutiennent par ailleurs que le RGPD et la loi du 30 juillet 2018 restent d'application et qu'il serait opportun que le texte le précise. Enfin, ils demandent un élargissement de l'application de l'avant-projet de loi, pouvant s'appliquer aux intermédiaires d'assurance, en plus des entreprises d'assurance et des entreprises de réassurance. Cela est justifié par le fait que, selon leur lecture du RGPD, ces intermédiaires ne sont pas des sous-traitants mais des responsables du traitement des données de santé[188].

Enfin, en ce qui concerne les experts, ces derniers mettent en lumière divers problèmes soulevés par l'insertion de la réglementation proposée dans la quatrième partie de la loi du 4 avril 2014 relative aux assurances. Ils estiment par ailleurs que l'avant-projet laisse planer un doute quant au maintien de l'application des autres droits et principes consacrés dans le RGPD et dans la loi 30 juillet 2018 sur la protection de la vie privée, ce qui crée de l'insécurité juridique. L'application de cette législation doit dès lors être clairement mentionnée[189].

---

[185] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L 119/1, 4 mai 2016, considérant n°52.

[186] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L 119/1, 4 mai 2016, art. 9.2, g).

[187] Avis de la Commission des assurances sur l'avant-projet de loi relatif au traitement des données à caractère personnel concernant la santé, Doc/C2021/3, 20 décembre 2021, p. 6 et 7.

[188] Avis de la Commission des assurances sur l'avant-projet de loi relatif au traitement des données à caractère personnel concernant la santé, Doc/C2021/3, 20 décembre 2021, p. 7 et 8.

[189] Avis de la Commission des assurances sur l'avant-projet de loi relatif au traitement des données à caractère personnel concernant la santé, Doc/C2021/3, 20 décembre 2021, p. 9.

La Commission des assurances approuve l'objectif général de la protection des données de santé, ainsi que le besoin de sécurité juridique, tant pour les assurés que pour les entreprises d'assurance et de réassurance. Ainsi, la Commission est d'avis que la suppression complète du consentement explicite et préalable comme base de traitement des données de santé rendrait toute une série de situations illégales (le traitement de ces données par les intermédiaires d'assurance, du bureau du suivi des assurances solde restant dû, les médecins-conseils, les avocats et par l'Ombudsman des assurances, par exemple). Pour cette raison, la Commission des assurances met en garde contre les ambiguïtés de la formulation de l'article 61/5, §1, alinéa 1er de l'avant-projet, pouvant laisser entendre que l'interdiction des données de santé serait à caractère absolu et non relatif. Dès lors, la Commission demande que le texte de loi et l'exposé des motifs prévoient clairement que le projet n'a pas pour objet d'entraver le traitement de ces données en vertu d'une autre base de traitement de l'article 9, §2 du RGPD et qu'il ne porte pas préjudice à la loi du 4 avril 2014 (articles 58 et 61), à la législation relative aux droits du patient et au règlement en matière de gestion des données relatives à la santé par le médecin-conseil de l'assureur. Ainsi, la Commission invite le Ministre à réviser de manière approfondie les différents articles de l'avant-projet de loi[190].

L'étude de l'avis de la Commission des assurances a deux apports. En premier lieu, elle permet d'avoir une vision globale du débat concernant l'importance du consentement explicite et préalable pour les consommateurs et la demande d'une plus grande souplesse juridique à cet égard de la part des assureurs. L'avis est intéressant, car il permet également de souligner les faiblesses de l'argumentaire des délégations des assureurs. En effet, par exemple, selon le Dr. Régis Radermecker, secrétaire général de l'Association du diabète, dans une expertise, la longueur des procédures n'est pas due à l'exigence de consentement explicite et préalable, mais au caractère contradictoire de ces procédures et à la consolidation de l'état du patient[191]. De même, les justifications apportées par le Ministre de l'Économie – à savoir la protection des intérêts des assurés par le biais de l'octroi d'une mission d'intérêt public à l'assureur – semblent ignorer les intérêts commerciaux sous-jacents des assureurs.

[190] Avis de la Commission des assurances sur l'avant-projet de loi relatif au traitement des données à caractère personnel concernant la santé, Doc/C2021/3, 20 décembre 2021, p. 11 à 20.
[191] P. LALOUX, « Les assureurs veulent accéder à certaines données de santé sans consentement », disponible sur www.lesoir.be, 21 janvier 2022.

En second lieu, l'étude de cet avis permet d'avoir une vision globale des enjeux juridiques à la fois particuliers et généraux qui concernent la protection des données de santé et le droit à l'information des assureurs. Les enjeux juridiques particuliers concernent les arguments juridiques en faveur ou en défaveur du maintien du consentement explicite et préalable comme base de traitement des données de santé. Les enjeux juridiques généraux concernent la particularité des données concernant la santé, le rapport entre la protection des données à caractère personnel et la protection de la vie privée, ainsi que la transversalité du droit (droit de l'Union européenne, droit belge et jurisprudence de la Cour eur. D.H.).

Nous pouvons donc voir que l'avant-projet de loi dont il est question suscite une levée de boucliers de la part d'associations de consommateurs et de patients. C'est le cas de l'Association du diabète qui estime que ce dernier constitue une menace pour la protection des données et pour le secret médical, et est en contrariété avec le RGPD et la CEDH. Suite aux nombreuses critiques dont a fait l'objet le projet, le 25 janvier 2022, le Ministre a décidé d'y renoncer[192]. Dès lors, le consentement explicite de la personne concernée demeure toujours à l'heure actuelle la seule base de traitement possible des données de santé dans le domaine des assurances en Belgique. En effet, il n'est toujours pas certain que les fondements de l'article 9, §2, b), g), h) et i) permettent de justifier le traitement des données de santé par les assureurs, sous réserve, toutefois, d'un éclaircissement de leur portée par la CJUE à l'avenir[193].

Toujours dans l'analyse de l'exigence du consentement explicite, le cas luxembourgeois mérite une attention particulière dans une perspective de droit comparé. Avant l'adoption du RGPD, l'article 7, §3 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel prévoyait que « le traitement de données relatives à la santé nécessaire aux fins de la gestion de services de santé peut être mis en œuvre notamment par les compagnies d'assurance lorsque le responsable de traitement est soumis au secret professionnel »[194]. À la suite de l'adoption du RGPD, la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du RGPD remplace la loi de 2002, mais ne prend pas de formule similaire pour légitimer le

[192] L. CRENIER et R. RADERMECKER, « Abandon de l'avant-projet Dermagne ! », disponible sur www.diabete.be, 25 janvier 2022.
[193] J.-M. BINON, *op. cit.*, p. 1963.
[194] Chambre des salariés Luxembourg, « avis III/29/2020 relatif au projet de loi relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances », disponible sur www.csl.lu, 28 mai 2020, p. 2.

traitement des données de santé par les assureurs. Dès lors, le consentement explicite de la personne concernée est la seule base de traitement possible des données de santé par les compagnies d'assurance luxembourgeoises. Cette base de traitement reçoit les mêmes critiques qu'en Belgique, à savoir qu'elle ne constitue pas une base juridique fiable et solide pour le traitement des données de santé, et que le consentement « pourrait ne pas être considéré comme libre au sens du RGPD pour certains types d'assurance (p.ex. assurance-vie dans le contexte d'un prêt hypothécaire, assurance solde restant dû,…) [195]». Pour remédier à l'insécurité juridique dans laquelle se trouvent les compagnies d'assurance luxembourgeoises, à l'instar de la Belgique, un projet de loi est rédigé en vue d'introduire, dans la loi sur le secteur des assurances, une disposition qui légitimise le traitement des données de santé par les compagnies d'assurance en se basant, conformément à l'article 9, §2, g) du RGPD, sur des motifs d'intérêt public important. Par un avis du 27 janvier 2020, la Commission nationale pour la protection des données approuve ce projet de loi, estimant qu'il « énumère de manière suffisante quelles sont [les] mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée qui sont à respecter en cas de traitement des données de santé nécessaires à l'exécution de mesures précontractuelles en matière d'assurance ou de réassurance ou à l'exécution d'un contrat d'assurance ou de réassurance »[196], mais, contrairement à la Commission des assurances belge, elle propose de supprimer le consentement explicite de la personne concernée comme base de traitement des données de santé en assurances. *A contrario*, la Chambre des salariés du Luxembourg, dans un avis du 28 mai 2020, désapprouve ce projet de loi, estimant que les compagnies d'assurance poursuivent avant tout un but de lucre, et ne poursuivent que partiellement un intérêt public, d'ailleurs réservé aux assurés qui ont les moyens de conclure de telles assurances[197]. Elle conclut en disant que « cet article n'est rien d'autre qu'une farce et permet aux compagnies d'assurance qui sont

[195] Commission nationale pour la protection des données du Grand-Duché de Luxembourg, « avis de la Commission nationale pour la protection des données relatif au projet de la loi n°7511 relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances », disponible sur www.cnpd.public.lu, 27 janvier 2020, p. 2.

[196] Commission nationale pour la protection des données du Grand-Duché de Luxembourg, « avis de la Commission nationale pour la protection des données relatif au projet de la loi n°7511 relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances », disponible sur www.cnpd.public.lu, 27 janvier 2020, p. 3.

[197] Chambre des salariés Luxembourg, « avis III/29/2020 relatif au projet de loi relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances », disponible sur www.csl.lu, 28 mai 2020, p. 6.

à la fois juge et partie du traitement des données des assurés de disposer comme bon leur semble »[198]. Comme en Belgique, ce projet de loi n'a finalement pas abouti.

L'enjeu de la deuxième Section réside dans le fait d'expliciter le rôle des assurances dans le traitement des données de santé qui est multidimensionnel. En effet, d'une part le monde des assurances a fait montre d'une certaine adaptation afin de se conformer aux exigences d'une protection accrue des données de santé. Mais paradoxalement, les assurances sont aussi celles qui, du fait notamment d'une relation asymétrique qui existe entre celles-ci et les preneurs d'assurance, sont susceptibles d'être la source de la violation des droits et libertés des preneurs. En ce sens, les demandes d'allègement de la condition de consentement explicite de la part des assurances ont reçu un accueil mitigé en Belgique.

Au sein de ce Chapitre, nous avons souhaité présenter l'état de droit en matière de protection des données de santé et le rapport avec les assurances, celles-ci étant des responsables de traitement du sens du RGPD. Nous l'avons vu, le RGPD apporte une harmonisation et une précision qui sont attendues en matière de données de santé, au sein d'une société qui est plus connectée que jamais. Elle laisse le soin aux États membres d'adapter les dispositions du RGPD pour instituer un régime de protection plus important encore. En ce sens, des législations nationales ont effectivement pu préciser le champ d'application du RGPD. Pour autant, il serait erroné de croire que toutes les situations de traitement de données à caractère personnel reçoivent désormais une réponse appropriée et surtout univoque. En effet, que cela soit du fait de l'inventivité des responsables de traitement comme les assurances ou de la tendance même de traiter les données dans un monde ultra-connecté, de nombreuses situations de traitement de données sont soit des cas limites, soit des violations banalisées du régime de protection des données à caractère personnel.

[198] Chambre des salariés Luxembourg, « avis III/29/2020 relatif au projet de loi relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances », disponible sur www.csl.lu, 28 mai 2020, p. 6.

## Chapitre 2. Une étude de trois cas limites illustrant les ambiguïtés du régime de la protection des données de santé dans le monde des assurances

Nous allons nous concentrer, au sein du Chapitre 2, sur quelques-uns de ces cas limites recouvrant la situation du recours aux détectives privés par les compagnies d'assurance (**section 1**), le cas spécifique de la médecine d'assurance (**section 2**), et enfin, les défis d'aujourd'hui et de demain concernant les données recueillies par les objets connectés (**section 3**).

### Section 1. Du recours aux détectives privés par les assurances et de la manipulation des données de santé

Un article du journal *Le Soir* datant de 2022 recense 750 détectives agréés en Belgique. Environ 400 d'entre eux travaillent pour des compagnies d'assurance[199]. La raison pour laquelle les compagnies d'assurance engagent des détectives privés est la crainte de la fraude à l'assurance qui constitue une de leurs préoccupations principales. Selon Insurance Europe, le coût des fraudes détectées en Europe s'élève à 2,5 milliards d'euros en 2017, et en Belgique à plus de 500 millions d'euros par an[200]. Assuralia estime que le coût de la fraude à l'assurance R.C. automobile représente 120 à 140 millions d'euros par an, ce qui a pour conséquence que les automobilistes payent une prime d'assurance de 3% à 6% plus chère que nécessaire, soit l'équivalent de 150 euros par an[201]. Quant à la France, selon un sondage réalisé par YouGov, le pourcentage de Français avouant avoir commis une fraude à l'assurance est passé de 11% à 20% en 2022[202]. En assurance maladie, le directeur général de la Caisse nationale d'Assurance maladie, Thomas Fatôme, indique que le coût de la fraude représente 315 millions d'euros en 2022. Aussi, l'argument selon lequel la fraude à l'assurance est un fléau pesant financièrement sur les assurés honnêtes est retrouvé de manière répétée chez les assureurs, ainsi que chez une partie de la doctrine. Il est intéressant de noter qu'un ancien responsable des assurances de Test-Achats s'interroge sur la pertinence des chiffres relatifs à la fraude à l'assurance et trouve dès lors l'argument faible.

---

[199] F. DELEPIERRE, « Le vrai ou faux : les entreprises publiques font-elles appel à des détectives privés ? », disponible sur www.lesoir.be, 25 décembre 2022.
[200] Insurance Europe, « Insurance fraud : not a victimless crime », disponible sur www.insuranceeurope.eu, novembre 2019.
[201] Assuralia, « Les assureurs unissent leurs efforts dans la lutte contre la fraude. Création d'une banque de données sinistres : une primeur pour le secteur de l'assurance », disponible sur www.assuralia.be, 25 janvier 2021.
[202] H. TORREANI, « La fraude à l'assurance a doublé en 2022 ! », disponible sur www.lelynx.fr, 30 juin 2022.

Pour remédier à la fraude, les compagnies d'assurance ont recours à des détectives privés afin de vérifier les circonstances de survenance d'un sinistre, l'ampleur des dommages subis et la bonne foi de l'assuré. Le fondement d'un traitement de données personnelles en matière de lutte contre la fraude relève de l'intérêt légitime de l'assureur au sens de l'article 6, §1, f) du RGPD. En effet, le considérant 47 du RGPD vise expressément la prévention de la fraude comme constituant un intérêt légitime du responsable de traitement. À ce titre, aussi bien l'exploitation de données collectées initialement pour une autre fin, telle que l'appréciation du risque, que l'exploitation de données collectées aux fins de débusquer une fraude sont licites[203]. Toutefois, pour ce faire, les détectives privés utilisent des méthodes parfois très intrusives qui portent atteinte à la vie privée des assurés[204].

La profession de détective privé fait l'objet d'un encadrement juridique éclectique. Elle est réglementée par la loi du 19 juillet 1991[205] et ses arrêtés, mais est également soumise à la réglementation en matière de protection de la vie privée et des données à caractère personnel vue *supra*[206]. Ces réglementations ont donc pour effet de limiter le champ d'activité et les moyens d'action du détective privé.

Il est entendu par détective privé « toute personne physique qui, dans un lien de subordination ou non, exerce habituellement, contre rémunération et pour le compte d'autrui, des activités »[207] énumérées dans la présente loi ou dans les arrêtés délibérés en Conseil des ministres consistant, notamment, à « réunir des éléments de preuve ou constater des faits qui donnent ou peuvent donner lieu à des conflits entre personnes ou qui peuvent être utilisés pour mettre fin à ces conflits »[208]. Pour pouvoir exercer la profession de détective privé, il est nécessaire d'obtenir une autorisation du Ministre de l'Intérieur[209]. En outre, le détective devra respecter les conditions d'exercice du chapitre 3 de la loi, établir une convention écrite avec son client assureur qui comprend une « description précise de la mission confiée »[210], mentionner sa qualité de détective dans tous les documents qu'il émet[211], ainsi que remettre à son client, à la

[203] D. COCTEAU-SENN, A. CHARPENTIER et R. BIGOT, « La protection des données personnelles en assurance – dialogue du juriste avec l'actuaire », disponible sur www.f-origin.hypotheses.org, p. 12 et 13.
[204] D. V., « Détectives privés en assurance », disponible sur www.compareil.fr, 31 août 2021.
[205] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991.
[206] C. LEDUC, « La preuve d'une fraude à l'assurance : comment mener au mieux l'enquête ? », *Bull. ass.*, 2018/1, n°402, p. 6.
[207] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 1, §1.
[208] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 1, §1, 3.
[209] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 2 et 3.
[210] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 8.
[211] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 11.

fin de sa mission, un rapport qui doit comporter une série d'éléments[212] dont seuls son client et les personnes mandatées par ce dernier peuvent prendre connaissance[213].

Dans la loi du 19 juillet 1991, il existe par ailleurs des limitations quant aux domaines d'enquête du détective privé. En ce qui nous intéresse dans le cadre de ce mémoire, la loi « interdit au détective privé de recueillir des informations relatives à la santé […] des personnes qui font l'objet de ses activités »[214]. La *ratio legis* de l'article 7 de la loi de 1991 est de compléter la protection offerte par le secret médical[215]. En effet, dans les travaux préparatoires de la loi, il est possible de lire que « la protection du secret médical n'est sans doute en effet pas suffisante pour empêcher un détective privé de recueillir des informations relatives à la santé des personnes et à les divulguer au client. Il s'agit là d'une atteinte intolérable à la vie privée des individus »[216]. Dès lors, nous pouvons en déduire qu'il est interdit au détective privé d'accéder au dossier médical d'un patient, à un rapport médical, et de manière plus générale, à tout fichier contenant des données de santé[217]. De plus, le Tribunal du travail de Liège, dans un jugement du 23 novembre 2017, indique qu'il ne convient pas d'interpréter l'article 7, alinéa 3 de la loi du 19 juillet 1991 restrictivement, l'interdiction ne portant pas uniquement sur la collecte de données de santé couvertes par le secret médical, mais sur la collecte de données de santé au sens large[218].

La question se pose alors de savoir si la surveillance, par un détective privé, des faits et gestes d'une personne dans un lieu accessible au public pour en déduire des informations sur son état de santé, telle que sa réelle mobilité, afin de détecter une éventuelle fraude est licite[219].

Il est intéressant de noter que les travaux préparatoires de la loi de 1991 cantonnent les agissements du détective privé au respect de la vie privée. Cependant, la notion de « vie privée »

[212] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 9.
[213] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 10, al. 1.
[214] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 7, al. 3.
[215] D. MOUGENOT, « Humphrey Bogart au XXI^e siècle : la preuve par production d'un rapport de détective privé », note sous C. trav. Liège, 15 décembre 2008, *Rev. rég. dr.*, p. 253.
[216] Projet de loi organisant la profession de détective privé, discussion des articles, *Doc. Sén.*, 1990-1991, n°1259/2, p. 36.
[217] I. REUSENS, « De quelques modes de preuve en droit de la responsabilité à la lumière de la protection de la vie privée », *Droit de la responsabilité*, I. Reusens (dir.), 1^ère éd., Bruxelles, Larcier, 2015, p. 32.
[218] Trib. trav. Liège, 23 novembre 2017, R.G. n°16/6623/A, disponible sur www.terralaboris.be.
[219] I. REUSENS, *ibidem*, p. 30.

est une notion complexe, polysémique et difficile à définir en droit[220]. L'article 22 de la Constitution, combiné avec l'article 8 de la CEDH, forment l'assise juridique sur laquelle s'établit la notion de droit au respect de la vie privée[221]. Aussi, la Cour eur. D.H. précise, au fil de sa jurisprudence, les contours et l'étendue de cette notion incertaine, ainsi que les effets qu'elle emporte en droit.

La notion de vie privée étant définie de manière extrêmement large par la Cour eur. D.H., une surveillance dans un lieu public peut constituer une violation de l'article 8 de la CEDH. Toutefois, le droit au respect de la vie privée n'est pas un droit absolu. Des dérogations sont possibles, pour autant qu'elles respectent les exigences de légalité, de légitimé et de proportionnalité de l'alinéa 2 de l'article 8 de la CEDH. Le recours à un détective privé parait rencontrer l'exigence de légalité, l'article 1 de la loi du 17 juillet 1991 disposant qu'une des activités du détective privé consiste à « réunir des éléments de preuve ou constater des faits qui donnent ou peuvent donner lieu à des conflits entre personnes ou qui peuvent être utilisés pour mettre fin à ces conflits »[222]. Quant à l'exigence de légitimité, cette dernière parait également être rencontrée. En effet, la Cour du travail d'Anvers, se fondant sur l'article 8 de la CEDH, juge légitime pour un assureur de se prémunir des fraudes commises par ses assurés[223]. Par ailleurs, la Cour eur. D.H. juge que l'assureur a le droit de faire des enquête privées afin de vérifier si les conditions de l'assurance sont remplies[224]. L'exigence de proportionnalité est pour sa part plus délicate. En vertu du principe de proportionnalité, une ingérence dans la vie privée est autorisée, pour autant qu'elle soit strictement limitée à ce qui est nécessaire pour atteindre le but poursuivi. Une surveillance 24 heures sur 24 ne respecterait donc pas l'exigence de proportionnalité[225]. Nous constatons que la jurisprudence de la Cour eur. D.H et la jurisprudence belge sont casuistiques par rapport à cette exigence. Il n'est pas possible de déduire que toute surveillance dans un lieu public est autorisée de manière automatique. Il s'agit de procéder à chaque fois à une appréciation des circonstances propres de l'espèce[226]. En tout

[220] Cour eur. D.H., « Guide sur l'article 8 de la Convention – Droit au respect de la vie privée et familiale, du domicile et de la correspondance, disponible sur www.echr.coe.int, mis à jour au 31 août 2022, p. 26.
[221] Parlement européen, « Le droit au respect de la vie privée : les défis digitaux, une perspective de droit comparé – Belgique», disponible sur www.europarl.europa.eu, octobre 2018, p. 5.
[222] Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 1, §1, 3.
[223] C. trav. Anvers, 1er octobre 2002, *R.W.*, 2002-2003, p. 298.
[224] Cour eur. D.H., arrêt *Verlière c. Suisse*, 28 juin 2001, p. 6.
[225] D. MOUGENOT, *op. cit.*, p. 250 ; *voy.*, par exemple, C. trav. Mons, 22 mai 2007, *R.D.T.I.*, 2008, p. 239 considérant que les moyens mis en œuvre par le détective privé, à savoir la surveillance 24 heures sur 24 et 7 jours sur 7 d'un travailleur et de sa compagne afin de vérifier que le travailleur n'utilisait pas son véhicule de travail à des fins personnelles, étaient disproportionnés par rapport à la finalité.
[226] D. MOUGENOT, *op. cit.*, p. 248 à 250.

état de cause, dans un arrêt du 17 janvier 2019, la Cour eur. D.H. considère que le recours à un détective privé par une compagnie d'assurance en vue de vérifier le bien-fondé de la demande en réparation de la victime ne constitue pas une violation de l'article 8 de la CEDH lorsque cette méthode s'impose par l'objectif poursuivi au motif que « les investigations de l'assureur, effectuées à partir du domaine public et limitées à la constatation de la mobilité du requérant, visaient uniquement à préserver les droits patrimoniaux de l'assurance »[227] et que « les informations éparses, recueillies par hasard et sans aucune pertinence pour l'investigation, étaient loin de constituer une collecte systématique ou pertinente »[228].

Il est de doctrine et de jurisprudence plus ou moins constante qu'une déduction sur l'état de santé d'une personne faite sur la base d'une photo ou d'une vidéo prise par un détective privé dans un lieu accessible au public ne constitue pas une donnée relative à la santé, ce constat n'étant pas soumis au secret médical étant donné qu'il est constatable par tous, et s'agissant d'une déduction, n'étant pas directement relatif à la santé de la personne[229]. À titre exemplatif, un jugement récent du Tribunal de première instance francophone de Bruxelles considère qu' « en décrivant les sorties et les déplacements de la victime sur des voies accessibles au public, les détectives privés mandatés par la compagnie d'assurance ne recueillent pas des informations relatives à l'état de santé, au sens de l'article 7 de la loi du 19 juillet 1991 »[230]. Le tribunal indique par ailleurs que « s'il fallait considérer que l'article 7 de la loi précitée interdit toute collecte et description d'informations sur les modes de déplacement de la personne surveillée, ainsi que sur son emploi du temps et ses activités, dès lors qu'elle pourrait avoir une incidence sur l'appréciation des séquelles dont la personne surveillée reste affectée à la suite d'un accident, et donc, sur son état de santé, cela exclurait de façon quasi systématique l'intervention d'un détective privé pour procéder à des constatations sur les activités d'une personne dans le but que soit vérifié, sur cette base et sur celles des autres éléments d'un dossier, si l'incapacité dont elle fait état se vérifie en pratique »[231].

---

[227] Cour eur. D.H., arrêt *Elvir Mehmedovic et Eldina Mehmedovic c. Suisse*, 17 janvier 2019, §17.
[228] Cour eur. D.H., arrêt *Elvir Mehmedovic et Eldina Mehmedovic c. Suisse*, 17 janvier 2019, §18.
[229] L. VAN GOSSUM, note sous C. trav. Bruxelles, 18 mars 2002, *Bull. Ass*., 2002, p. 645 ; C. LEDUC, *op. cit*., p. 15 ; D. MOUGENOT, *ibidem*, p. 253 ; I. REUSENS, *op. cit*., p. 32 ; Civ. fr. Bruxelles (87e ch.), 11 janvier 2021, *J.T*., 2021, p. 333 ; Mons (22e ch.), 7 janvier 2020, *For. Ass*., n°211, 2021, p. 41 ; Civ. Charleroi, 1er octobre 2020, R.G., n°14/3360/A, *inédit* ; Trib. trav. Hainaut, div. Tournai, 19 janvier 2018, R.G. n°14/504/A, disponible sur www.terralaboris.be ; C. trav. Bruxelles (6e ch.), 9 juin 2017, *For. Ass*., 2018, p. 95 ; C. trav. Bruxelles (5e ch.), 18 mai 2015, n° 2014/AB/996 ; C. trav. Mons, 4 novembre 2013, R.G. n°2011/AM/397, disponible sur www.juridat.be ; Civ. Anvers, 7 mars 2007, R.W., 2008-2009, p. 332.
[230] Civ. fr. Bruxelles (87e ch.), 11 janvier 2021, *J.T*., 2021, p. 333.
[231] Civ. fr. Bruxelles (87e ch.), 11 janvier 2021, *J.T*., 2021, p. 334.

Un arrêt de la Cour du travail de Liège du 15 décembre 2008 statue toutefois en sens contraire. En l'espèce, il est question d'un assureur qui, suspectant une fraude, mandate un détective privé pour que ce dernier prouve que la motricité d'une victime d'un accident est nettement moins déficiente que ce qu'établit l'expertise judiciaire[232]. La Cour écarte le rapport du détective privé qui avait suivi la victime en présence d'un huissier de justice, considérant que « des informations sur la question de savoir si les fonctions d'une personne sont, ou ne sont pas, troublées par une maladie ou par une lésion, constituent des informations relatives à la santé »[233]. Ici, la Cour reproche au détective privé d'avoir décrit de manière excessivement détaillée la motricité de la personne, ce qui s'assimile à une collecte d'informations relatives à la santé[234]. Selon Dominique Mougenot, il est probable que la Cour n'arrive pas à la même conclusion avec un rapport moins détaillé sur la manière dont la personne se déplace[235]. Cet arrêt fait l'objet de nombreuses critiques de la part d'une frange de la doctrine[236], notamment parce qu'il ne tient pas compte de la distinction opérée par les articles 9 du RGPD et 34 de la loi du 30 juillet 2018 entre les données qui permettent de déduire une information relative à la santé et les données qui contiennent l'information relative à la santé, étant entendu que seul le traitement de ces dernières est prohibé[237].

La question de la validité juridique des écrits que les détectives privés produisent à l'issue de leurs enquêtes se pose aussi. Il nous importe de rappeler que le rapport d'un détective privé n'a pas force probante authentique et n'est pas un mode de preuve irréfutable. Depuis l'adoption de la loi du 19 juillet 1991, il n'est plus contesté que le rapport de détective privé peut constituer un mode de preuve au titre de présomption de l'homme au sens de l'article 1349 de l'ancien Code civil[238]. Sa valeur probante dépendra donc fortement des circonstances. Il en résulte dès lors un pouvoir d'appréciation important dans le chef du juge qui, en vertu de l'article 1353 de l'ancien Code civil, ne peut admettre que des présomptions graves, précises et concordantes. Le juge doit donc se montrer prudent en tenant compte de la présence ou non d'autres éléments de preuve corroborant le rapport, du caractère légal, loyal, fiable ou non et unilatéral du rapport,

[232] D. MOUGENOT, *op. cit*., p. 251 et 252.
[233] C. trav. Liège, 15 décembre 2008, *R.R.D*., 2008, n°127, p. 251.
[234] C. LEDUC, *op. cit*., p. 15.
[235] D. MOUGENOT, *ibidem*, p. 252.
[236] S. GILSON et C. MENIER, « Les conditions d'admissibilité de la preuve par détective privé », obs. sous. Mons (22e ch.), 14 janvier 2020, *For. Ass*, n° 211, 2021, p. 37 ; C. LEDUC, *op. cit*., p. 15 ; D. MOUGENOT, *op. cit*., p. 253 ; I. REUSENS, *op. cit*., p. 32.
[237] S. GILSON et C. MENIER, *ibidem*, p. 37.
[238] *Voy*. Par exemple : Mons (22e ch.), 16 juin 2020, *Bull. ass*., liv. 3, p. 369 ; Mons (22e ch.), 14 janvier 2020, *For. Ass*., n°211, 2021, p. 41 ; Mons (22e ch.), 7 janvier 2020, *For. Ass*., n°211, 2021, p. 41 ; Mons (22e ch.), 4 décembre 2018, *R.G.A.R*., 2019/2, p. 15551.

ainsi que des conditions dans lesquelles l'enquête a eu lieu[239]. Ce mode de preuve est donc licite, pour autant qu'il respecte la réglementation relative à la profession de détective privé, ainsi que la réglementation relative à la vie privée et aux données à caractère personnel[240].

Toutefois, en cas de violation de ces réglementations, se pose alors la question de savoir si la jurisprudence dite « Antigone » de la Cour de cassation permettrait d'accueillir une preuve recueillie de manière illégale ou irrégulière par un détective privé.

Depuis un arrêt de principe de la Cour de cassation du 12 mars 1923[241], confirmé à maintes reprises[242], une preuve recueillie illégalement, ainsi que toutes les preuves qui en découlent directement et indirectement, sont considérées comme entachées de nullité, et doivent dès lors être écartées des débats[243]. Toutefois, en 2003, un important revirement de jurisprudence est opéré. En effet, la Cour de cassation, par l'arrêt *Antigone*[244], autorise qu'une preuve recueillie de manière irrégulière puisse être prise en considération « à condition qu'aucune règle de forme prescrite à peine de nullité n'ait été méconnue, que l'irrégularité commise n'ait pas entaché la fiabilité de la preuve et que l'usage de la preuve ne compromette pas le droit au procès équitable »[245]. Par un arrêt du 23 mars 2004, la Cour de cassation renforce sa jurisprudence en obligeant dorénavant le juge à admettre une preuve recueillie de manière irrégulière en dehors des trois cas précités [246]. En outre, dans cet arrêt, la Cour de cassation énumère une série de critères pouvant être pris en considération pour apprécier l'admissibilité de la preuve recueillie de manière illicite, critères qui sont complétés dans son arrêt *Manon* du 2 mars 2005[247]. Cette jurisprudence est ultérieurement suivie par d'autres juridictions. Ainsi, par exemple, la Cour constitutionnelle affirme dans deux arrêts qu'une preuve obtenue en violation du droit au respect de la vie privée n'est pas automatiquement nulle[248]. Ces arrêts étant rendus en matière pénale, la doctrine s'interroge sur leur transposition aux matières civiles. À la suite d'un arrêt

[239] D. MOUGENOT, *op. cit*., p. 243.
[240] I. REUSENS, *op. cit*., p. 27.
[241] Cass., 12 mars 1923, *Pas*., 1923, p. 233.
[242] *Voy*. Cass., 10 mai 1965, *Pas*., 1965, p. 952 ; Cass., 15 février 1965, *Pas*., 1965, p. 601 ; Cass., 29 octobre 1962, *Pas*., 1963, p. 272 ; Cass., 13 octobre 1952, *Pas*., 1953, p. 52 ; Cass., 2 septembre 1948, *Pas*., 1948, p. 488 ; Cass., 24 mai 1948, *Pas*., 1948, p. 334 ; Cass., 6 mars 1944, *Pas*., 1944, p. 237 ; Cass., 3 février 1941, *Pas*., 1941, p. 30 ; Cass., 4 mars 1929, *Pas*., 1929, p. 118.
[243] I. REUSENS, *op. cit*., p. 47.
[244] Cass., 14 octobre 2003, R.G. n°P.03.0762.N., disponible sur www.juridat.be.
[245] I. REUSENS, *op. cit*., p. 48.
[246] I. REUSENS, *ibidem*, p. 48.
[247] Cass., 2 mars 2005, *J.T*., 2005, p. 211.
[248] C.C., 27 juillet 2011, n°139/2011 ; C.C., 22 décembre 2010, *J.L.M.B*., 2011, p. 298.

de la Cour de cassation rendu le 10 mars 2008[249] dans une affaire de nature sociale contenant dans son dispositif des motifs similaires à ceux des arrêts *Antigone* et *Manon*, une majorité d'auteurs considèrent que la jurisprudence Antigone s'applique également aux matières civiles et sociales. Toutefois, étant donné que cet arrêt concerne une infraction à une réglementation d'ordre public sanctionnée pénalement, certains auteurs émettent des doutes quant à l'application de cette jurisprudence à des litiges opposant des intérêts purement privés, se demandant si son domaine d'application ne se limite pas à tout ce qui touche à l'ordre public[250]. Les juridictions du travail sont d'ailleurs mitigées quant à l'application de cette jurisprudence[251]. Selon Claire Leduc, ces doutes ne sont pas fondés dans les litiges civils relatifs à l'existence d'une fraude à l'assurance établie au moyen de preuves obtenues par détectives privés étant donné que la fraude est une infraction pénale. Dès lors, ces litiges ne concernent pas que des intérêts privés[252]. Ainsi, le droit au respect de la vie privée n'étant pas un droit absolu, une preuve obtenue en violation de ce droit peut être admise comme présomption de l'homme en vertu de la jurisprudence *Antigone*[253]. De même, une preuve obtenue en violation de la loi du 19 juillet 1991 peut être admise comme présomption de l'homme par application des principes dégagés par cette jurisprudence[254].

En se basant sur la jurisprudence *Antigone*, des juridictions admettent la recevabilité des preuves recueillies par un détective privé en violation de l'article 7 de la loi du 19 juillet 1991 qui prohibe la collecte de données de santé par les détectives privés. À cet égard, nous pouvons citer un jugement du Tribunal du travail de Charleroi qui accueille un rapport et des images vidéos réalisés par un détective privé qui sont entachés d'irrégularités, ces irrégularités consistant en la violation des articles 11 (absence de mention du numéro d'autorisation d'exercer la profession) et 7 (enquête sur la capacité d'une personne à se déplacer sans béquille) de la loi du 19 juillet 1991[255], considérant, après avoir effectué le test « Antigone », que « le recours au droit de la vie privée ne peut justifier que des faits observés sur la voie publique par un détective privé et qui apparaissent contradictoires avec ceux constatés peu auparavant à l'expertise judiciaire, ne soient pas soumis à l'appréciation de l'expert d'abord et du juge ensuite si les principes du contradictoire et de la proportionnalité ont été respectés ». Nous

[249] Cass., 10 mars 2008, *J.L.M.B*., 2009, p. 580.
[250] C. LEDUC, *op. cit*., p. 39.
[251] S. GILSON et C. MENIER, *op. cit.*, p. 40.
[252] C. LEDUC, *op. cit*., p. 39.
[253] C. LEDUC, *ibidem*, p. 40.
[254] I. REUSENS, *op. cit*., p. 51.
[255] Trib. trav. Charleroi (1ère ch.), 16 juin 2010, *Bull. Ass*., 2010/3, p. 292.

pouvons également citer un jugement du Tribunal du travail de Liège qui, sur base de la même motivation que le jugement précité, accueille un rapport de détective privé et des images prises par ce dernier violant le prescrit de l'article 7 de la loi du 19 juillet 1991 (enquête sur les capacités fonctionnelles de l'assuré à la suite de son accident du travail)[256].

Bien que l'article 7 de la loi du 19 juillet 1991 interdise la collecte de données de santé par les détectives privés, nous pouvons donc constater que dans la pratique, des détectives privés recueillent illégalement des données de santé qui, grâce à la jurisprudence *Antigone*, sont admises comme moyen de preuve en justice.

Il reste pertinent de dresser un parallèle avec la situation française. En principe, la Cour de cassation française suit la ligne jurisprudentielle de la Cour eur. D.H. et consacre la recevabilité de la preuve par enquête privée, causant une atteinte au droit au respect de la vie privée dès lors qu'une telle atteinte est proportionnée au but poursuivi. En effet, dans un arrêt du 31 octobre 2012[257] et selon une jurisprudence alors bien établie, la Cour de cassation considère l'enquête contestée comme étant recevable. En l'espèce, une personne revendique la nécessité de bénéficier d'une assistance permanente en raison de sa perte d'autonomie, tandis que l'enquête privée démontre que cette personne est apte à conduire un véhicule. Aussi, « la position habituelle de la Cour de cassation […] était fondamentalement de permettre l'exercice d'un droit à la preuve de la fraude par l'assureur pourvu que ce droit soit contrebalancé par un principe de proportionnalité de nécessité de l'information recueillie »[258]. Cependant dans deux arrêts du 25 février 2016[259] et du 17 mars 2016[260], la Cour de cassation affirme une position nettement plus stricte en estimant que des investigations se déroulant sur plusieurs années portent une atteinte disproportionnée, et ce faisant, ne peuvent constituer une preuve recevable dans le cadre d'une enquête pour fraude à l'assurance.

Pour terminer, il est à noter que selon des articles de presse récents, la Ministre de l'Intérieur, Annelies Verlinden, aurait pour projet de modifier la loi du 19 juillet 1991 pour mieux encadrer la profession de détective privé et ses activités au regard des exigences du RGPD et des

[256] Trib. trav. Liège, 23 novembre 2017, R.G. n°16/6623/A, disponible sur www.terralaboris.be.
[257] Cass. (1re civ.), 31 octobre 2012, n°11-17.476, disponible sur www.legifrance.gouv.fr.
[258] J. SPERONI, « Fraude à l'assurance : le monde rêvé de la Cour de cassation », disponible sur www.argusdelassurance.com, 7 juillet 2016.
[259] Cass. (1re civ.), 25 février 2016, n°15-12.403, disponible sur www.legifrance.gouv.fr.
[260] Cass. (1re civ.), 17 mars 2016, n°15-11.412, disponible sur www.legifrance.gouv.fr.

nouvelles technologies à disposition des détectives privés qui ont évolué depuis l'adoption de cette loi[261].

Ainsi, au sein de cette première Section, nous avons souhaité revenir sur le régime juridique des détectives privés dans le droit belge en rapport avec le respect de la vie privée et notamment la protection des données de santé. Si une réforme du régime juridique est souhaitée par la Ministre de l'Intérieur, nous pouvons en déduire que le régime juridique actuel n'est plus adapté aux évolutions technologiques que connait cette profession, et manque de clarté – et probablement d'effectivité – par rapport à l'interdiction de collecter des données de santé en raison de la jurisprudence *Antigone*. Il nous a également paru important de rappeler d'une part, le rôle certain que joue la Cour eur. D.H. dans la définition de la vie privée et d'autre part, le caractère avant tout jurisprudentiel de notre cas d'étude. Il est en outre intéressant de voir que ces aspects sont en constante évolution.

## Section 2. Une analyse du statut ambigu des médecins-conseils au contact privilégié des données de santé

Quand il s'agit de la protection des données de santé, le statut du médecin d'assurance mérite une attention bien particulière. Œuvrant pour les assureurs, la manipulation des données de santé par de tels médecins appelle à un encadrement d'autant plus important que la relation entre assureurs et preneurs d'assurance est asymétrique. Or, les cas de violations relayés par la presse ou les insuffisances du cadre législatif existant posent question. Pour comprendre ces points, nous allons exposer dans un premier temps quelques ambiguïtés inhérentes au statut du médecin-conseil (**§1**) avant de s'attarder sur des situations de violation de la protection des données de santé (**§2**) et, enfin, d'exposer les interprétations de l'APD en la matière (**§3**).

[261] F. DELEPIERRE, « Le vrai ou faux : les entreprises publiques font-elles appel à des détectives privés ? », disponible sur www.lesoir.be, 25 décembre 2022 ; F. DE HALLEUX, « Les détectives privés ne peuvent pas tout faire : la ministre Verlinden va les recadrer ! », disponible sur www.sudinfo.be, 19 décembre 2022.

## §1. Un détour par les ambigüités inhérentes au statut du médecin-conseil

Les médecins-conseils de compagnie d'assurance sont des praticiens professionnels qui ont pour mission de déterminer l'état de santé d'un candidat à l'assurance, d'un assuré ou d'un tiers lésé[262]. Le statut du médecin-conseil est défini par l'article 43 du Code de déontologie médicale[263]. Plusieurs législations nous renseignent quant aux obligations du médecin-conseil. Nous pouvons citer celles qui nous semblent les plus pertinentes à l'égard de notre sujet. Ainsi, les médecins-conseils sont soumis à la loi relative aux droits du patient[264] qui s'applique aux rapports juridiques, de droit privé ou de droit public, en matière de soins de santé dispensés à un patient par un praticien professionnel[265]. Cette loi définit le praticien professionnel comme « le praticien visé à l'arrêté royal n°78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé ainsi que le praticien professionnel ayant une pratique non conventionnelle, telle que visée dans la loi du 29 avril 1999 relative aux pratiques non conventionnelles dans les domaines de l'art médical, de l'art pharmaceutique, de la kinésithérapie, de l'art infirmier et des professions paramédicales »[266]. Quant aux soins de santé, ils sont définis comme les « services dispensés par un praticien professionnel en vue de promouvoir, de déterminer, de conserver, de restaurer ou d'améliorer l'état de santé d'un patient, de modifier son apparence corporelle à des fins principalement esthétiques ou de l'accompagner en fin de vie »[267]. Les médecins-conseils de compagnie d'assurance sont également soumis à la loi relative à la qualité de la pratique des soins de santé[268] qui est applicable « aux professionnels des soins de santé dans le cadre de la prestation de soins de santé »[269], les soins de santé étant définis de la même manière que dans la loi relative aux droits du patient[270]. En outre, ils sont soumis à la loi relative aux assurances[271], en particulier l'article 61 qui dispose que « l'examen médical, nécessaire à la conclusion et à l'exécution du contrat, ne peut être fondé que sur les antécédents déterminant l'état de santé actuel du candidat-assuré et non sur des techniques d'analyse génétique propres à déterminer

[262] I. LUTTE, « L'accès aux données de santé. À propos du dossier médical établi par le médecin-conseil d'une compagnie d'assurance », *Rev. dr. santé*, n°3, 2020, p. 260.
[263] Code de déontologie médicale, art. 43.
[264] Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 20 décembre 2002.
[265] Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 20 décembre 2002, art. 3.
[266] Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 20 décembre 2002, art. 2, 3°.
[267] Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 20 décembre 2002, art. 2, 2°.
[268] Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B.*, 14 mai 2019.
[269] Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B.*, 14 mai 2019, art. 3.
[270] Loi coordonnée du 10 mai 2015 relative à l'exercice des professions des soins de santé, *M.B.*, 18 juin 2015, art. 2, 3°.
[271] Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014.

son état de santé futur »[272]. Par ailleurs, cet article indique que le médecin-conseil joue un rôle de filtre, étant donné que « ce dernier ne peut communiquer aucune information non pertinente eu égard au risque pour lequel les certificats ont été établis ou relative à d'autres personnes que l'assuré »[273]. En outre, l'article dispose que « lorsqu'il n'existe plus de risque pour l'assureur, le médecin-conseil restitue, à leur demande, les certificats médicaux à l'assuré ou, en cas de décès, à ses ayants droits »[274]. Traitant de données médicales, les médecins-conseils sont également soumis à la réglementation en matière de protection de la vie privée et des données à caractère personnel. Enfin, ils se doivent de respecter le Code de déontologie médicale[275]. Ainsi, ces législations multiples ne nous donnent qu'une vision parcellaire du statut des médecins-conseils et rendent difficile l'appréhension d'un régime juridique unifié et harmonisé.

En ce qui concerne le médecin-conseil d'assureurs mutualistes, son statut est également défini par l'arrêté royal 35 du 20 juillet 1967[276], par la loi du 11 avril 1995 visant à instituer « la charte » de l'assuré social[277], ainsi que par la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994[278]. Ce dernier exerce une fonction officielle après avoir prêté serment devant le Comité du Service d'évaluation et de contrôle médicaux (ci-après « SECM ») de l'INAMI. Le SECM émet des directives dans le chef des médecins-conseils afin de préciser leurs droits et obligations. Par ailleurs, les médecins-conseils sont soumis aux médecins-directeurs ainsi qu'à la direction médicale de leur organisme assureur, mais les mesures disciplinaires relèvent de la compétence du SECM et non de l'Ordre des médecins[279]. Alors conseiller au sein de l'INAMI, Serge Hostaux qualifie expressément le statut du médecin-conseil d'« hybride »[280]. L'hybridité est illustrée par le fait que le médecin-conseil a une relation contractuelle tout en ayant des obligations statutaires, et du fait de la particularité de ses

[272] Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, art. 61, al. 3.
[273] Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, art. 61, al. 2.
[274] Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, art. 61, al. 5.
[275] Conseil national de l'Ordre des médecins, « force obligatoire du Code de déontologie médicale », disponible sur www.ordomedic.be, 16 juin 2018.
[276] Arrêté royal 35 du 20 juillet 1967 portant le statut et le barème des médecins-conseil chargés d'assurer auprès des organismes assureur le contrôle médical de l'incapacité primaire et des prestations de santé en vertu de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, *M.B.*, 29 juillet 1967.
[277] Loi du 11 avril 1995 visant à instituer « la charte » de l'assuré social, *M.B.*, 6 septembre 1995.
[278] Loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, *M.B.*, 27 août 1994 ; S. HOSTAUX, *Le droit de l'assurance soins de santé indemnités*, 1ère éd., Bruxelles, Larcier, 2009, p. 288.
[279] Cellule stratégique de la Ministre des Affaires sociales et de la Santé publique, « Pacte d'avenir avec les organismes assureurs », disponible sur www.ocm-cdz.be, septembre 2016, p. 26.
[280] Serge HOSTAUX, *op. cit.*, p. 288.

fonctions, le médecin-conseil conserve une certaine forme d'indépendance dans le contenu de sa mission, tout en dépendant des assurances et de la SECM[281].

En-dehors de cette question de subordination, l'ambiguïté se situe également autour du statut du médecin-conseil à l'égard des patients. L'idée qu'il pourrait exister un risque d'asymétrie concernant les informations communiquées aux assurances et aux patients fait débat. En effet, notamment dans le cadre de l'évaluation de l'incapacité de travail, les médecins-conseils sont amenés à manipuler des données sensibles. Il lui appartient en effet de constituer le dossier médical[282], lequel comprend les données médicales de la personne évaluée[283]. Par ailleurs, un avis de l'Observatoire des maladies chroniques intitulé « la relation patient – médecin conseil » se fonde sur une enquête réalisée par la LUSS, qui est la fédération francophone des associations des patients et de proches et le porte-parole des usagers des services de santé[284]. Cette enquête met notamment en avant le fait que le droit à la protection de la vie privée n'est pas toujours respecté en pratique, et cela est d'autant plus avéré que certains médecins-conseils ne se sentent pas liés par les obligations découlant de la loi relative aux droits du patient[285]. L'Observatoire émet des recommandations pour remédier à cette situation, comme l'octroi de formations visant à sensibiliser sur les droits des patients. Cela fait écho à un élément de notre entretien avec un médecin généraliste ayant déjà agi comme médecin-conseil pour certains de ses patients dans le cadre d'actions en responsabilité médicale. Selon ses dires, les médecins sont très peu informés sur les obligations que leur imposent la loi et le Code de déontologie médicale en ce qui concerne leurs relations avec les compagnies d'assurance. Ce médecin généraliste trouve d'ailleurs souhaitable qu'un Groupe local d'évaluation médicale (GLEM) soit organisé afin qu'ils soient mieux informés sur les obligations légales et déontologiques leur incombant à cet égard.

[281] Serge HOSTAUX, *ibidem*, p. 289.
[282] Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B*, 14 mai 2019, art. 34.
[283] INAMI, « IV. Directives aux médecins conseil pour l'organisation du contrôle et de l'évaluation de l'incapacité de travail », disponible sur www.inami.fgov.be, 2015/3, p. 35.
[284] Courrier de l'Observatoire des maladies chroniques au Président/à la Présidente du comité SECM *et al*., le 20 août 2018 à Bruxelles, disponible sur www.inami.fgov.be.
[285] Courrier de l'Observatoire des maladies chroniques au Président/à la Présidente du comité SECM *et al*., le 20 août 2018 à Bruxelles, disponible sur www.inami.fgov.be, annexe 1, p. 2.

## §2. Des accès illicites au dossier médical de patient par des médecins-conseils

En 2019, un cas inédit de consultation abusive de dossier médical électronique de patient sur le Réseau Santé Wallon (ci-après « RSW ») est relaté. Un médecin chirurgien crée un lien thérapeutique avec une patiente pour accéder à des documents médicaux la concernant[286]. L'hôpital est responsable de la procédure à suivre afin d'établir un lien thérapeutique avec un patient[287]. Dans certains hôpitaux, la carte d'identité du patient est nécessaire à cet effet[288]. Dans le cas d'espèce, il a suffi pour le médecin de préalablement vérifier l'identité de ce dernier via le Registre national ou la plateforme « CareNet » pour qu'une relation thérapeutique puisse être créée[289].

La même année, le CSI autorise le fournisseur d'Helena, une plateforme permettant l'échange de données de santé entre médecins et patients, à diminuer le niveau de sécurité afin de faciliter l'accès par les patients à leur dossier médical, et par extension, à leurs données de pension et à leur historique de rémunération, de sorte qu'il était possible d'y accéder sans s'identifier au moyen d'une carte d'identité ou de l'application Itsme. Pour s'y connecter, il suffit d'entrer un code envoyé par mail, et confirmé par un médecin par sms[290]. L'identité du patient n'est donc pas certifiée par une instance officielle de l'État et rien ne permettait d'établir le lien thérapeutique avec le médecin dont émane le code[291]. Craignant une fuite des données de santé, Medispring, une coopérative de plus de 2.200 médecins, porte plainte auprès de l'APD contre la décision du CSI[292]. La coopérative présente une série de témoignages de médecins et de patients portant sur les risques liés à cet accès facilité (*e.g.*, usurpation de l'identité en vue de consulter son statut vaccinal)[293]. Cinq médecins et un patient se joignent à cette plainte[294]. Dans

[286] J. ROLDAN PEREZ, « Un médecin a consulté les dossiers médicaux en ligne de Claire, sans autorisation : « Il est remonté jusqu'en 2003 et il a tout pris » », disponible sur www.rtl.be, 9 avril 2019.
[287] PM, « Triste première : un médecin hospitalier consulte abusivement un dossier patient (RSW) », disponible sur www.lespecialiste.be, 8 avril 2019.
[288] C. VAN REETH, « Un médecin consulte les données médicales d'un ex-patient sans autorisation : un incident qui pose question », disponible sur www.lesoir.be, 8 avril 2019.
[289] PM, « Triste première : un médecin hospitalier consulte abusivement un dossier patient (RSW) », disponible sur www.lespecialiste.be, 8 avril 2019.
[290] Test-Achats, « Nos données privées de santé sont-elles suffisamment protégées ? », disponible sur www.test-achats.be, 10 novembre 2021.
[291] P. LALOUX, « Comment Frank Robben a ouvert une brèche dans l'accès à nos données santé et pension », disponible sur www.lesoir.be, 26 octobre 2021.
[292] BELGA, « Protection des données de santé dans l'app Helena : une plainte déposée à l'Autorité de protection des données », disponible sur www.rtbf.be, 27 octobre 2021.
[293] P. LALOUX, « « Helena « ne représente pas une menace pour vos données de pension. » Vraiment ? », disponible sur www.lesoir.be, 27 octobre 2021.
[294] BELGA, « Protection des données de santé dans l'app Helena : une plainte déposée à l'Autorité de protection des données », disponible sur www.rtbf.be, 27 octobre 2021.

les travaux préparatoires de la loi sur l'ADS, le Ministre fédéral de la Santé, Frank Vandenbroucke, indique que « l'application Helena n'a pas donné un accès illimité aux données de santé. Cette plate-forme était un moyen d'authentification conçu pour sécuriser la communication entre les patients et les prestataires de soins. Il y a eu un cas unique d'un seul médecin généraliste qui n'a pas suivi les procédure définies, avec le consentement d'un patient. Le médecin en question a ainsi pu se faire passer pour le patient concerné »[295]. Quand bien même il est question d'un cas isolé, un seul accès non autorisé suffit pour que cela soit considéré comme une violation de données au sens du RGPD[296], tout en laissant poindre le risque de violations futures. En effet, en principe, pour qu'un accès à des données de santé soit licite, il faut récolter le consentement préalable du patient et qu'il existe un lien thérapeutique entre le médecin et celui-ci[297]. Il est intéressant de remarquer que cette faille de sécurité ayant donné lieu au dépôt d'une plainte à l'APD est intervenue au moment où l'indépendance de l'APD est fortement remise en cause, et y est liée, étant donné que le CSI, et plus particulièrement Frank Robben, est à l'origine de cette décision. Nous renvoyons aux critiques formulées *supra* à l'encontre du CSI et ce qui était reproché à Frank Robben. Certains s'interrogent alors quant à la capacité de l'APD de traiter cette plainte dans ce contexte[298], une interrogation qui semble légitime. Pour s'en convaincre, il suffit de constater qu'il n'existe aucune trace du suivi de cette plainte par l'APD. Par la suite, Helena est suspendue le temps de réaliser une enquête[299]. Dans un communiqué, les responsables de la plateforme Helena tentent de rassurer les citoyens en affirmant qu'elle « est bien sécurisée et surveillée afin d'éviter tout abus »[300]. À présent, la plateforme Helena est toujours accessible, mais uniquement au moyen d'une carte d'identité ou de l'application Itsme[301].

[295] Projet de loi relatif à l'institution et à l'organisation de l'Agence des données de (soins de) santé, rapport de la première lecture fait au nom de la commission de la Santé et de l'Égalité des chances, *Doc., Ch*., 2022-2023, n° 3065/004, p. 28.
[296] P. LALOUX, « « Helena « ne représente pas une menace pour vos données de pension. » Vraiment ? », disponible sur www.lesoir.be, 27 octobre 2021.
[297] P. LALOUX, « Comment Frank Robben a ouvert une brèche dans l'accès à nos données de santé et pension », disponible sur www.lesoir.be, 26 octobre 2021.
[298] P. LALOUX, « Vie privée : Helena devrait prévenir tous ses patients d'une potentielle violation de leurs données de santé », disponible sur www.lesoir.be, 27 octobre 2021.
[299] BELGA, « L'Absym demande des éclaircissements sur la plateforme en ligne Helena », disponible sur www.rtbf.be, 28 octobre 2021.
[300] BELGA, « Plainte à l'APD au sujet d'Helena : Helena ne représente pas une menace, selon mypension.be », disponible sur www.numerikare.be, 27 octobre 2021.
[301] P. LALOUX, « Vie privée : Helena devrait prévenir tous ses patients d'une potentielle violation de leurs données de santé », disponible sur www.lesoir.be, 27 octobre 2021.

Dans la même logique, une autre affaire fait parler d'elle. En 2020, un article dans le journal flamand *De Morgen* relate que des médecins-conseils de compagnie d'assurance consultent à l'hôpital les dossiers médicaux électroniques de patients sans leur consentement afin d'obtenir des informations relatives à leurs antécédents médicaux en vue de contester des remboursements dans certains dossiers. *De Morgen* a recueilli plusieurs témoignages de patients dans ce sens. Parmi ces témoignages, l'un relate même la modification d'un rapport médical dans un sens favorable à la compagnie d'assurance[302].

Ces cas relayés par les médias mettent en lumière des données de santé convoitées, ainsi que des cas de violations de la protection des données de santé. Toutefois, la presse est loin de rendre compte de tous les agissements *contra legem* existants[303].

Les conditions de consentement et de lien thérapeutique desquelles dépend la licéité de l'accès aux données de santé sont définies par le législateur. Les articles 36 à 40 de la loi relative à la qualité de la pratique des soins de santé régissent l'accès aux données de santé par des professionnels des soins de santé. L'article 36 exige le consentement éclairé du patient préalablement à tout accès par un professionnel des soins de santé « aux données à caractère personnel relatives à la santé du patient qui sont tenues à jour et conservées par d'autres professionnels des soins de santé »[304]. La charge de la preuve de ce consentement repose sur le professionnel de soins de santé[305]. Le consentement éclairé et préalable du patient n'est toutefois pas requis en cas d'urgence médicale[306].

En outre, seul le professionnel des soins de santé qui entretient une relation thérapeutique avec le patient a accès aux données de santé de ce dernier[307]. La relation thérapeutique est définie comme « toute relation entre un patient et un professionnel des soins de santé dans le cadre de laquelle des soins de santé sont dispensés »[308]. Ainsi, la médecine d'assurance entre en principe dans la définition de la relation thérapeutique qui est très large[309]. En effet, dans les travaux

---

[302] C. GALLE, « Verzekeringsartsen kunnen meekijken in uw medisch dossier », disponible sur www.demorgen.be, 23 janvier 2020.
[303] I. LUTTE, « Le dossier médical et les données de santé sous le prisme de la « loi qualité », *Revue belge du dommage corporel et de médecine légale*, 2021/2, p. 60.
[304] Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B.*, 14 mai 2019, art. 36.
[305] I. LUTTE, « Le dossier médical et les données de santé sous le prisme de la « loi qualité », *op. cit.*, p. 60.
[306] Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B.*, 14 mai 2019, art. 39.
[307] Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B.*, 14 mai 2019, art. 37, al. 1.
[308] Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B.*, 14 mai 2019, art. 37, al. 2.
[309] I. LUTTE, *op. cit.*, p. 61.

préparatoires de la loi concernée, nous lisons que « la relation peut être de nature diagnostique, curative, préventive ou palliative, mais, par exemple, la médecine d'entreprise, la médecine des assurances et la médecine de contrôle relèvent en principe également de la définition de la relation thérapeutique »[310]. Toutefois, l'accès aux données de santé du patient par l'ensemble des professionnels des soins de santé relevant de la définition de la relation thérapeutique n'est, dans certains cas, pas compatible avec la finalité de l'échange desdites données de santé. En effet, si l'échange des données de santé a pour finalité le traitement préventif et curatif du patient, il y a lieu d'exclure la médecine d'assurance, la médecine de contrôle et la médecine légale qui se bornent à établir un diagnostic[311]. Dès lors, le texte prévoit qu'un arrêté royal peut désigner les catégories de professionnels des soins de santé, qui, bien qu'ayant une relation thérapeutique avec un patient, ne peuvent pas avoir accès à ses données de santé[312]. À cet égard, les travaux préparatoires de la loi font expressément référence à l'exclusion de la médecine des assurances, la médecine de contrôle, ainsi que la médecine légale qui n'établissent qu'un diagnostic et qui n'agissent pas préventivement ni de manière curative[313]. Pour l'heure, cet arrêté royal n'a pas encore été adopté, ce que regrette l'APD (*voy*. *infra*).

Par ailleurs, la loi énumère trois conditions qu'un professionnel des soins de santé qui entretient une relation thérapeutique avec un patient doit respecter pour avoir accès à ses données de santé : « 1° la finalité de l'accès consiste à dispenser des soins ; 2° l'accès est nécessaire à la continuité et à la qualité des soins de santé dispensés ; 3° l'accès se limite aux données utiles et pertinentes dans le cadre de la prestation de soins de santé »[314]. Dès lors, le professionnel des soins de santé n'a accès qu'aux données de santé nécessaires à la santé du patient et non dans l'intérêt d'un tiers tel qu'un assureur, et, s'agissant de données sensibles, doit les manipuler avec prudence, étant donné que leur traitement est par principe interdit[315].

Si la médecine d'assurance entre dans la définition de la relation thérapeutique dans la loi relative à la qualité de la pratique des soins de santé, le Conseil national de l'Ordre des médecins n'est toutefois pas du même avis. En effet, dans un avis du 15 février 2020, le Conseil indique

[310] Projet de loi relatif à la qualité de la pratique des soins de santé, commentaire des articles, *Doc., Ch*., 2018-2019, n°3441/001, p. 51.
[311] I. LUTTE, *op. cit*., p. 61.
[312] Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B*., 14 mai 2019, art. 37, al. 3.
[313] Projet de loi relatif à la qualité de la pratique des soins de santé, commentaire des articles, *Doc., Ch*., 2018-2019, n°3441/001, p. 52.
[314] Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B*., 14 mai 2019, art. 38.
[315] I. LUTTE, *op. cit*., p. 61 et 62.

que le médecin-conseil d'une compagnie d'assurance n'entretient pas une relation thérapeutique avec la personne dont il est chargé d'évaluer l'état de santé, et ne peut dès lors accéder à un des réseaux d'échange des données de santé régionaux tels que le Réseau santé Bruxellois, le RSW, CoZo, etc.[316]. À cet égard, un médecin généraliste nous a fait part, lors d'une interview, de ses craintes concernant l'accès aux réseaux d'échange des données de santé par les médecins d'assurances. Bien qu'ils ne puissent pas y avoir accès déontologiquement parlant, il leur est techniquement possible d'y accéder au moyen de la carte d'identité du patient, étant donné que certains médecins-conseils de compagnie d'assurance sont par ailleurs des médecins généralistes. Ces craintes sont également partagées par l'ancien responsable des assurances de Test-Achats.

### §3. Une critique émanant de l'APD revenant sur les limites de la protection des données de santé

Dans une recommandation du 16 mai 2017, le Comité sectoriel de la sécurité sociale et de la santé section « santé » dénonce déjà les limites du traitement des données de santé contenues dans le dossier de patient avec la finalité de traitement de ces données par le médecin-conseil qui réalise une expertise médicale du patient pour le compte d'un tiers, tel qu'un assureur. Le médecin-conseil qui réalise une telle expertise doit avoir préalablement obtenu le consentement du patient et l'avoir préalablement informé de sa qualité, de sa mission, ainsi que des personnes qui accéderont à ses données de santé[317]. Par ailleurs, le Comité indique que tout hôpital est tenu d'obliger les médecins de déclarer leur activité de médecin-conseil, et d'ensuite bloquer leur accès aux données de santé du patient concerné[318]. Dans un avis sollicité par la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration, l'APD est amenée à se prononcer au sujet de la conformité de la loi relative à la qualité de la pratique des soins de santé au RGPD, en particulier ses articles 36 et suivants concernant l'accès aux données de

[316] Conseil national de l'Ordre des médecins, « Accès aux données médicales d'une personne par le médecin chargé d'évaluer son état de santé », disponible sur www.ordomedic.be, 15 février 2020.
[317] Comité sectoriel de la sécurité sociale et de la santé (section « santé »)», « Recommandation n°17/01 du 16 mai 2017 relative à l'incompatibilité entre le rôle de prestataire de soins ayant une relation thérapeutique et le rôle de médecin-conseil, contrôleur ou expert à la demande d'un tiers à l'égard du même patient », disponible sur www.ehealth.fgov.be, 16 mai 2017, p. 2.
[318] Le Comité sectoriel de la sécurité sociale et de la santé (section « santé »), « Recommandation n°17/01 du 16 mai 2017 relative à l'incompatibilité entre le rôle de prestataire de soins ayant une relation thérapeutique et le rôle de médecin-conseil, contrôleur ou expert à la demande d'un tiers à l'égard du même patient », disponible sur www.ehealth.fgov.be, 16 mai 2017, p. 3 et 4.

santé[319]. La Ministre interroge l'APD plus particulièrement sur la portée du consentement des articles 36 et suivants de la loi, et sur la mise en œuvre technique de droits d'accès de professionnels des soins de santé dans des systèmes électroniques et télématiques[320]. En ce qui concerne la portée du consentement, l'APD relève que l'exposé des motifs de la loi relative à la qualité de la pratique des soins de santé précise qu' « il ne s'agit pas d'un consentement dans le cadre duquel les professionnels de santé bénéficiant d'un accès sont désignés par le patient individuel. En revanche, le texte prévoit expressément que le patient peut exclure certains professionnels des soins de santé lorsqu'il donne son consentement »[321]. Dès lors, l'APD en déduit qu'étant donné que les données du patient peuvent être partagées avec d'autres professionnels des soins de santé, sauf ceux que le patient exclut expressément, il s'agit d'un consentement général[322].

Cependant, la question du consentement éclairé ou non se pose en pratique. En effet, dans une enquête de 2019, l'Institut de microélectronique et composants (ci-après « IMEC ») relève qu'il existe une différence importante entre le nombre de consentements officiellement enregistrés cette année-là (82%) et le nombre de citoyens interrogés indiquant dans le questionnaire avoir donné leur consentement éclairé à l'échange numérique des données de santé entre professionnels des soins de santé (46,3% et 51,7% en Flandre). L'IMEC indique que cette différence peut s'expliquer par le fait que les patients donnent leur consentement machinalement et dans la précipitation, par exemple en cochant une case, et ne se souviennent plus l'avoir donné explicitement. Selon l'IMEC, cette différence peut également s'expliquer par le fait que consentir à l'échange de leurs données de santé n'est pas vu comme une décision fondamentale, mais va, au contraire, de soi. L'IMEC affirme en tout état de cause qu'il est absolument indispensable d'informer les patients sur la signification de ce consentement et sur la possibilité de le retirer à tout moment[323]. Quant à la possibilité d'empêcher un professionnel

[319] Autorité de protection des données, « Traitement de données provenant de dossiers de patients – Demande d'avis de la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration », disponible sur www.autoriteprotectiondonnees.be, DOS-2019-04611.
[320] Autorité de protection des données, « Traitement de données provenant de dossiers de patients – Demande d'avis de la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration », disponible sur www.autoriteprotectiondonnees.be, DOS-2019-04611, p. 2.
[321] Projet de loi relatif à la qualité de la pratique des soins de santé, commentaire des articles, *Doc., Ch.*, 2018-2019, n°3441/001, p. 50.
[322] Autorité de protection des données, « Traitement de données provenant de dossiers de patients – Demande d'avis de la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration », disponible sur www.autoriteprotectiondonnees.be, DOS-2019-04611, p. 3 et 4.
[323] IMEC, « ehealthmonitor 2019 – Résumé », disponible sur www.gcm.rmnet.be, p. 7 et 8.

des soins de santé d'accéder au dossier médical d'un patient, Test-Achats explique que bien que cette exclusion soit prévue par la loi, elle n'est pas toujours possible en pratique[324].

L'APD précise toutefois que l'exclusion de professionnels des soins de santé conformément à l'article 36, alinéa 2 de la loi ne doit en aucun cas porter préjudice au bon fonctionnement de l'hôpital ni empêcher de dispenser des soins de santé de qualité. En effet, l'exclusion ne concerne que l'accès aux données de santé du patient enregistrées par d'autres professionnels des soins de santé, ce qui n'empêche pas un professionnel des soins de santé ayant fait l'objet d'une telle exclusion de dispenser des soins de santé ni d'enregistrer et de traiter les données de santé du patient nécessaires à cet effet[325].

Quant au droit d'accès par un professionnel des soins de santé aux données tenues à jour et conservées par un autre professionnel des soins de santé, l'APD est d'avis que ce droit d'accès doit faire l'objet d'un encadrement renforcé, à savoir, *a minima*, l'exclusion de la médecine d'assurance, de la médecine de contrôle et de la médecine légale. En outre, elle recommande de prévoir la possibilité d'exclure et d'autoriser nominativement et des catégories de professionnels des soins de santé en veillant à la validité de la durée d'accès, ainsi que la mise en œuvre d'une notification préalable faite au patient afin qu'il puisse donner son consentement librement et en parfaite connaissance de cause. Ces limitations additionnelles doivent se faire *via* l'adoption d'arrêtés d'exécution dont l'application en pratique doit être contrôlée[326]. L'APD conclut qu'une intervention du Roi telle que prévue aux articles 36 et 37 de la loi est absolument indispensable, d'une part pour préciser la portée du consentement et sa mise en œuvre, d'autre part pour exclure de l'accès au dossier de patient (dont l'accès a essentiellement une finalité préventive et curative) la médecine d'assurance, la médecine de contrôle et la médecine légale (dont la finalité est seulement de diagnostiquer). Elle estime en effet que ces deux finalités sont totalement incompatibles avec le principe de limitation des finalités[327]. L'APD souligne

[324] B. JANSSEN et M. VAN HECKE, « Données médicales en ligne : comment les gérer vous-même ? », disponible sur www.test-achats.be, juin/juillet 2022.
[325] Autorité de protection des données, « Traitement de données provenant de dossiers de patients – Demande d'avis de la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration », disponible sur www.autoriteprotectiondonnees.be, DOS-2019-04611, p. 5.
[326] Autorité de protection des données, « Traitement de données provenant de dossiers de patients – Demande d'avis de la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration », disponible sur www.autoriteprotectiondonnees.be, DOS-2019-04611, p. 4 et 5.
[327] Autorité de protection des données, « Traitement de données provenant de dossiers de patients – Demande d'avis de la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration », disponible sur www.autoriteprotectiondonnees.be, DOS-2019-04611, p. 3.

également la nécessité de mettre en œuvre un mécanisme de contrôle et de surveillance de l'accès au dossier de patient[328].

Au sein de cette Section, nous avons souhaité exposer les risques de violation des données de santé inhérents à la profession de médecin-conseil. Bien que des législations existent, il semble qu'une approche extensive de la relation thérapeutique et les difficultés d'informer adéquatement le patient des enjeux de son consentement fragilisent une protection effective des données de santé. Cela est d'autant plus pressant que notre société n'a jamais été aussi connectée, rendant les données de santé vulnérables, susceptibles d'être exposées à grande échelle[329].

## Section 3. Une analyse prospective sur les objets connectés : de la digitalisation de l'assurance vers l'assurance connectée ?

Dans cette Section, il s'agira dans un premier temps d'illustrer (**§1**) et d'analyser l'impact de l'utilisation d'objets connectés par les assurances sur le modèle traditionnel de la mutualisation des risques (**§2**). Dans un troisième temps, il sera question d'étudier les balises mises en place par le législateur belge pour prévenir les dérives que pourrait entrainer l'utilisation d'objets connectés dans les assurances (**§3**). Dans un quatrième et dernière temps, nous examinerons, dans une perspective de droit comparé, le cadre juridique actuel de la France (**§4**).

### §1. Des illustrations sur l'impact de l'usage des objets connectés par les assurances sur la gestion des données de santé

Une montre connectée, une voiture connectée, une maison connectée voire une même ville connectée : il n'est aujourd'hui pas possible de nier que les objets connectés (ou *Internet of Things* (IoT)), protéiformes, font partie de notre quotidien. Leur usage s'est démultiplié au cours de ces dernières années, la pandémie ayant joué un rôle certain à cet égard. Aussi, en Belgique, l'IBPT, le régulateur du marché des télécoms, souligne qu'« [e]n 2021, le nombre d'objets

[328] Autorité de protection des données, « Traitement de données provenant de dossiers de patients – Demande d'avis de la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration », disponible sur www.autoriteprotectiondonnees.be, DOS-2019-04611, p. 7.
[329] L. DASINIERES, « Protection des données médicales, discrimination aux soins : les risques de Mon Espace Santé », disponible sur www.numerama.com, 7 janvier 2022.

connectés dépassait les 5 millions »[330]. En France, ce chiffre avoisine les 60 millions[331]. Fascinants et inquiétants à la fois, ces objets connectés créent de nouveaux défis juridiques, nous invitant même à repenser notre modèle sociétal. En ce sens, il est pertinent de comprendre quels sont leurs enjeux et conséquences en matière de santé et d'assurances. Avant cela, il importe de commencer par quelques illustrations.

En matière automobile, les assurances recourent déjà à des objets connectés. Nous pouvons renvoyer au dispositif « Pay How You Drive » qui consiste en un boitier électronique installé dans la voiture afin de récolter des informations relatives aux habitudes de conduite de l'assuré (nombre de kilomètres parcourus, temps passé au volant, manière de freiner et d'accélérer). Nous retrouvons le même procédé en France avec le contrat « Youdrive » de Direct Assurance et au Royaume-Uni avec le contrat « Rate my drive » d'Aviva Insurance. L'objectif de ce système d'assurance R.C. automobile est de proposer une prime d'assurance ajustée au type de conduite de l'assuré, s'avérant surtout intéressant pour les profils de risque réputés comme mauvais, comme les jeunes conducteurs, qui payent une prime d'assurance disproportionnée par rapport à leur réel profil de risque[332]. À cet égard, en France, la CNIL, souhaitant favoriser l'innovation tout en protégeant les données personnelles des usagers, élabore un pack de conformité « véhicules connectés » qui énonce des lignes directrices en la matière à l'attention des responsables de traitement concernés, leur permettant de se conformer à la loi Informatique et Libertés et au RGPD[333].

L'utilisation d'objets connectés dans les assurances de personnes, comme l'assurance maladie et l'assurance vie, pose davantage question, les données collectées étant des données de santé. Se développent de plus en plus les objets connectés et applications mesurant le mode de vie et l'état de santé des individus. Ceux-ci constituent une source d'informations précieuse pour les assureurs. Ils ne sont toutefois pas sans risque pour leurs utilisateurs, notamment sur le plan de la vie privée.

[330] A. MARTIN, « Les objets connectés et la conso de données s'envolent », disponible sur www.lecho.be, 9 juin 2022.
[331] X, « Combien pèse le marché des objets connectés en France ? », disponible sur www.boursorama.com, 3 juillet 2022. Il faut cependant se montrer prudent à l'égard de ces chiffres, qui varient selon la définition donnée aux objets connectés lors d'une étude, définition pour laquelle il n'existe pas de consensus.
[332] X, « Pay how you drive », disponible sur www.compare-assurance.be, *s.d.*, consulté le 23 juillet 2023.
[333] CNIL, « Pack de conformité : véhicules connectés et données personnelles », disponible sur www.cnil.fr, p. 2.

Une étude de 2020 réalisée par Test-Achats révèle que sur quatorze applications de nutrition et de santé analysées, seule une application est respectueuse de la réglementation en matière de protection de la vie privée. Il s'agit d'« Apple Health », qui est la seule application qui ne partage pas les données qu'elle collecte avec des tiers. Les autres partagent les données personnelles de leurs utilisateurs, telles que l'adresse e-mail, le nom et le sexe, avec des tiers. « Migraine Buddy » et « Sleep Cycle » envoient quant à elles des données relatives à la santé de leurs utilisateurs sans leur demander leur consentement et sans possibilité pour eux de s'y opposer. Test-Achats soulève le risque que ces données soient communiquées à des assureurs qui les opposeraient à leurs clients pour refuser de conclure un contrat d'assurance ou pour leur imposer une prime d'assurance plus élevée. Test-Achats porte dès lors plainte à l'APD pour violation du RGPD par quatre de ces applications[334].

La compagnie d'assurance américaine John Hancock est la première compagnie d'assurance à offrir des assurances santé liées aux objets connectés. En 2016, cette dernière propose un contrat d'assurance décès intégrant le programme Vitality lié à un objet connecté, tel qu'une Apple Watch ou un bracelet Fitbit. Par le biais de ce programme, la compagnie d'assurance peut évaluer l'hygiène de vie de ses assurés et les récompenser par des réductions sur des sites Internet ou dans des grands magasins, ainsi que par des réductions de prime d'assurance pouvant aller jusqu'à 15% de la prime annuelle en cas de bons résultats[335]. En 2018, la compagnie d'assurance John Hancock étend le programme Vitality à l'ensemble des contrats d'assurance vie qu'elle propose[336]. Ce modèle est depuis importé en Europe. En effet, le groupe italien Generali lance sur le marché allemand le 1er juillet 2017 un contrat d'assurance Vitality proposant des réductions de prime d'assurance de 11% à 16% aux assurés prenant soin de leur santé grâce à des programmes personnalisés et un suivi sur mesure, et à la transmission de leurs données de santé via une application Android. Le groupe implémente par ailleurs le programme Vitality en France le 1er juillet 2017, mais le cadre juridique ne permettant pas de réduire la prime d'assurance des assurés en récompense de leur bonne hygiène de vie, il prend une autre forme. Il s'agit d'une assurance complémentaire santé intégrant le programme Vitality qui récompense les assurés ayant une vie saine par des réductions auprès de partenaires (Amazon, Fnac, Expedia, etc.). S'agissant d'un programme facultatif, chaque entreprise ayant souscrit une

[334] Test-Achats, « Applications nutrition & santé : protégez vos données privées », disponible sur www.test-achats.be, 23 janvier 2020.
[335] X, « Santé : les objets connectés sous la loupe des assureurs », disponible sur www.lesechos.fr, 29 août 2017.
[336] F. LIMOGE, « John Hancock, l'assureur américain qui traque la bonne santé de ses assurés », disponible sur www.argusdelassurance.com, 24 septembre 2018.

telle assurance pour couvrir son personnel est libre de le proposer ou non à ses employés qui sont libres d'y souscrire. Ce programme importé des États-Unis soulève la question de la protection des données de santé avec la crainte de la revente de celles-ci aux partenaires de Vitality, voire aux employeurs.

## §2. Les objets connectés et les assurances : vers un nouveau modèle de gestion du risque ?

Traditionnellement, le mécanisme d'assurance repose sur la mutualisation des risques, de sorte que les primes d'assurance versées par l'ensemble des assurés servent à financer les sinistres qui viennent à se réaliser au cours d'une période donnée[337]. Pour ce faire, l'assureur doit vérifier que les risques couverts sont suffisamment dispersés pour qu'une compensation entre les risques qui se réalisent et les risques qui ne se réalisent pas s'opère, à défaut de quoi l'assureur pourrait se retrouver en difficultés[338]. L'assureur doit donc évaluer les risques qui lui sont soumis, et les classer en (sous-)catégories homogènes afin de les tarifer de manière adéquate. Cette classification ou segmentation permet de différencier la prime ou la couverture d'assurance en fonction des caractéristiques particulières du risque à couvrir[339]. Cette segmentation ne pouvant être par définition qu'imparfaite, une certaine solidarité entre les assurés en résulte : les assurés qui présentent moins de risques financent la garantie de ceux qui en présentent le plus[340].

Or, ce modèle pourrait être ébranlé par l'avènement de l'assurance connectée où le service assurantiel serait assuré par un réseau d'objets connectés qui collectent et analysent les données de leurs utilisateurs[341]. En effet, l'utilisation, par les assureurs, de données provenant d'objets connectés pourrait radicalement modifier le paradigme actuel de l'assurance pour verser dans une logique d'hyperpersonnalisation du risque et d'hyper-responsabilisation de l'individu[342], mettant ainsi à mal le principe de la mutualisation des risques[343], la solidarité entre les assurés, et étant source de discriminations et d'exclusions.

---

[337] C. PARIS, *Manuel de droit des assurances*, 1ère éd., Bruxelles, Larcier, 2021, p. 13.
[338] C. PARIS, *ibidem*, p. 15.
[339] C. PARIS, *ibidem*, p. 17.
[340] T. DERVAL, « Les assureurs peuvent-ils utiliser les données issues d'objets connectés ? », disponible sur www.lecho.be, 10 mars 2021.
[341] J. PEROCHEAU, « Connectes : quels enjeux pour l'assurance ? », disponible sur www.insurancespeaker-wavestone.com, 14 octobre 2019.
[342] J.-M. BINON, *op. cit.*, p. 1967.
[343] Pour nuancer le propos selon lequel l'utilisation d'objets connectés en assurances mettrait fin au principe de la mutualisation, nous pouvons souligner que, dans le cadre du contrat d'assurance « Pay how you drive » par

L'utilisation des données récoltées par des objets connectés présente de nombreux avantages pour les assureurs. Tout d'abord, une telle utilisation permet de tarifer le risque *in concreto*, en fonction du comportement de l'assuré, ce qui a pour effet d'inciter les assurés à la prévention en vue d'obtenir une prime d'assurance plus réduite, diminuant ainsi l'aléa moral. Cette tarification personnalisée permet par ailleurs d'attirer les bons profils de risque. Par voie de conséquence, le nombre et la gravité des sinistres – et *de facto* le coût de l'indemnisation – s'en voient réduits. Ensuite, la collecte de données provenant d'objets connectés permet par extension de détecter des anomalies, et donc de prévenir les sinistres ou d'en limiter leur étendue. Enfin, la collecte de données *via* des objets connectés permet aux assureurs d'avoir une meilleure connaissance de leurs clients, de sorte à pouvoir leur offrir un service répondant à leurs attentes et de leur appliquer une prime d'assurance qui reflète le risque réel qu'ils représentent[344].

Le jumelage du contrat d'assurance à un objet connecté a pour corrélatif que les bons risques auront tendance à opter pour cette pratique afin de se voir imposer une prime d'assurance correspondant au risque réel qu'ils représentent, alors que les mauvais risques s'y opposeront. Ainsi, en plus de l'augmentation des mauvais risques chez les assureurs ne proposant pas de tels contrats d'assurance, les assurés qui refusent d'utiliser un objet connecté risquent de se voir opposer un refus d'assurance ou de se voir imposer des primes plus élevées[345].

En matière d'assurance de personnes, l'exploitation par les assureurs des données issues d'objets connectés mènerait à une segmentation abusive entre les individus en bonne santé et ceux en moins bonne santé[346] avec dès lors le risque de discriminations fondées sur l'état de santé[347], en perdant de vue que les inégalités socio-économiques se répercutent sur l'état de

exemple, le conducteur reste confronté à des risques indépendants de sa volonté, tels que le comportement des autres conducteurs et les conditions météorologiques.

[344] J. PEROCHEAU, « Connectes : quels enjeux pour l'assurance ? », disponible sur www.insurancespeaker-wavestone.com, 14 octobre 2019.

[345] X, « L'Internet des objets : De nouvelles perspectives pour les assureurs », disponible sur www.headmind.com, 20 mars 2019.

[346] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, *Doc*., Ch., 2019-2020, n°0263/001, p. 1.

[347] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, *Doc*., Ch., 2019-2020, n°0263/001, p. 5.

santé des individus[348]. Ainsi, ce changement de paradigme pénaliserait surtout les plus défavorisés qui n'ont pas les moyens d'adopter un mode de vie sain[349]. Par ailleurs, l'utilisation d'objets connectés aboutirait à un modèle fondé sur l'hyper-individualisation des risques où les assurés seraient considérés comme responsables de leur santé. Ceci semble perdre de vue que la mort et la maladie sont considérés comme des accidents affectant les individus indépendamment de toute responsabilité individuelle[350].

La sélection du risque grâce aux données issues d'objets connectés étant bien plus complète que le système du questionnaire médical[351], le risque que le secteur des assurances encourt avec l'assurance connectée est la déshumanisation du secteur si la prime d'assurance venait à être définie exclusivement par des algorithmes et plus par des médecins[352]. Ceci peut dès lors nous amener à nous interroger sur l'avenir du rôle des médecins-conseils de compagnies d'assurance au stade la conclusion du contrat.

En pratique, la majorité des assurés, souhaitant préserver leur vie privée, est réticente à l'idée de se soumettre à un objet connecté. En effet, d'après des études réalisées par La Poste et par Opinion Way en 2014, 75% des Français sont méfiants quant à la transmission de leurs données *via* des objets connectés[353].

Un équilibre est donc à trouver entre d'une part la protection des consommateurs et le respect de la réglementation, notamment celle sur la protection des données et de la vie privée, et d'autre part la liberté d'entreprise des acteurs de l'assurance et l'innovation[354].

---

[348] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, *Doc*., Ch., 2019-2020, n°0263/001, p. 6.
[349] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, rapport de la deuxième lecture fait au nom de la Commission de l'économie, de la protection des consommateurs et de l'agenda numérique, *Doc*., Ch., 2019-2020, n°0263/009, p. 9.
[350] G. FRUY, « Une santé déconnectée des assureurs », *Les pages*, n°93, 2020, p. 1.
[351] M. REDON, *L'assurance santé privée à l'épreuve des objets connectés*, Thèse, Université de Rennes 1, disponible sur www.theses.hal.science, 2021, p. 47.
[352] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, rapport de la première lecture fait au nom de la Commission de l'économie, de la protection des consommateurs et de l'agenda numérique, *Doc*., Ch., 2019-2020, n°0263/005, p. 12.
[353] J. PEROCHEAU, « Connectes : quels enjeux pour l'assurance ? », disponible sur www.insurancespeaker-wavestone.com, 14 octobre 2019.
[354] X, « L'Internet des objets : De nouvelles perspectives pour les assureurs », disponible sur www.headmind.com, 20 mars 2019.

## §3. Les balises mises en place par le législateur belge : la loi du 10 décembre 2020[355]

L'adoption de la loi du 10 décembre 2020 est liée au développement croissant d'objets connectés permettant de collecter des données relatives au mode de vie ou à l'état de santé de leurs utilisateurs, et est motivée par la crainte de leur utilisation dans le domaine de l'assurance santé[356], ce qui constitue déjà une réalité dans les pays anglo-saxons comme vu ci-dessus. En effet, comme nous l'avons déjà mentionné dans le précédent paragraphe, une telle utilisation soulève diverses questions épineuses : la protection de la vie privée des utilisateurs et de leurs données, l'avenir des assureurs et des intermédiaires d'assurance qui pourrait être mis en péril si les géants du numérique qui détiennent une quantité massive de données s'emparent du marché des assurances, et le basculement vers une approche basée sur l'hyper-individualisation des risques avec les effets néfastes que cela entrainerait[357].

En vue de protéger les consommateurs contre les dérives liées à l'utilisation par les assureurs d'objets connectés[358] et de renforcer la protection des données de santé dans les assurances de personnes[359], le législateur belge introduit dans la loi du 4 avril 2014 relative aux assurances un chapitre 3 intitulé « Données à caractère personnel concernant le mode de vie ou la santé de l'assuré issues d'objets connectés » qui comporte trois articles.

L'article 46/1 de la loi du 4 avril 2014 relative aux assurances définit le champ d'application du chapitre 3 de la loi. Ce dernier est applicable aux contrats d'assurance individuelle sur la vie, ainsi qu'aux contrats d'assurance maladie visé à l'article 201, §1 de la loi. Sont donc exclues du champ d'application de ce chapitre les assurances groupe, ainsi que les assurances accident[360].

---

[355] Loi du 10 décembre 2020 modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir dans le domaine de l'assurance maladie et de l'assurance individuelle sur la vie une restriction de traitement des données à caractère personnel concernant le mode de vie ou la santé issues des objets connectés, *M.B.*, 15 janvier 2021.
[356] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, *Doc.*, Ch., 2019-2020, n°0263/001, p. 1.
[357] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, rapport de la première lecture fait au nom de la Commission de l'économie, de la protection des consommateurs et de l'agenda numérique, *Doc.*, Ch., 2019-2020, n°0263/005, p. 4.
[358] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, rapport de la deuxième lecture fait au nom de la Commission de l'économie, de la protection des consommateurs et de l'agenda numérique, *Doc.*, Ch., 2019-2020, n°0263/009, p. 3.
[359] J.-M. BINON, *op. cit.*, p. 1967.
[360] J.-M. BINON, *ibidem*, p. 1967 et 1968.

L'article 46/2 de la loi du 4 avril 2014 relative aux assurances dispose, quant à lui, que lors de la conclusion d'un tel contrat, le refus du candidat à l'assurance d'acquérir ou d'utiliser un objet connecté qui collecte des données à caractère personnel relatives à son mode de vie ou sa santé ne peut en aucun cas mener à un refus d'assurance ou à une augmentation de la prime d'assurance[361]. La loi ne définit pas la notion d'objet connecté, de sorte à pouvoir tenir compte des évolutions technologiques, mais cette notion fait l'objet d'une définition officielle en France, celle d'« objet qui est capable, outre sa fonction principale, d'envoyer ou de recevoir des informations par l'intermédiaire d'un réseau de télécommunication »[362].

Enfin, l'article 46/3 dispose qu' « aucune segmentation ne peut être opérée sur le plan de l'acceptation, de la tarification et/ou de l'étendue de la garantie sur la base de la condition que le candidat assuré accepte d'acquérir ou d'utiliser un objet connecté qui récolte des données à caractère personnel concernant son mode de vie ou sa santé, accepte de partager des informations récoltées par un tel objet connecté, ni sur la base de l'utilisation par l'assureur de telles informations »[363].

Bien que l'intitulé de la loi du 20 décembre 2020 parle d'une restriction au traitement des données à caractère personnel relatives au mode de vie ou à la santé issues des objets connectés, il s'agit, en réalité, d'une réelle interdiction faite aux assureurs de récolter et de traiter de telles données qui se décline en deux volets, le premier visant à éviter que le candidat à l'assurance soit pénalisé s'il venait à refuser d'acquérir un objet connecté qui transmettrait à l'assureur de telles données, et le deuxième à éviter que l'assureur favorise un candidat à l'assurance qui accepterait d'acquérir un objet connecté et de transmettre à l'assureur les données que cet objet collecterait[364]. À l'origine, les auteurs de la proposition de loi proposent d'interdire expressément le traitement « d'informations récoltées par un capteur de santé, relatives au mode de vie ou à l'état de santé du preneur d'assurance »[365]. Toutefois, à la suite d'un amendement, cette interdiction expresse est abandonnée au profit de simples restrictions encadrant le traitement des données à caractère personnel relatives au mode de vie ou à l'état de santé de

[361] Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, art. 46/2.
[362] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, amendement, *Doc.*, Ch., 2019-2020, n°0263/004, p. 3 et 4.
[363] Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, art. 46/3.
[364] J.-M. BINON, *op. cit.*, p. 1968.
[365] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, *Doc.*, Ch., 2019-2020, n°0263/001, p. 7.

l'assuré collectées par un objet connecté. Cela se fait en estimant que l'article 9, §1 du RGPD fait déjà ressortir de manière suffisamment claire cette interdiction[366]. Aussi, les auteurs de la proposition de loi s'en expliquent par la volonté d'obtenir l'adhésion la plus grande possible en faveur de la proposition de loi[367]. Cela peut également s'expliquer par la préoccupation du législateur belge de ne pas s'écarter de la faculté offerte par l'article 9, §4 du RGPD qui autorise les États membres à introduire tout au plus une limitation concernant le traitement de données à caractère personnel concernant la santé[368].

Il est à noter que si des données récoltées par les objets connectés comme le nombre de pas, de calories, les heures de sommeil ne constituent pas en tant que tel des données de santé au sens du RGPD, leur combinaison avec d'autres données, telles que l'indice de masse corporelle, peut permettre de déduire des informations sur l'état de santé de la personne concernée[369].

Cette interdiction mène à s'interroger sur la légalité de la communication à l'assureur, lors de la souscription du contrat, de données de santé collectées par un objet connecté utilisé par un médecin. À cet égard, Assuralia craint que l'interdiction établie par la loi ait pour conséquence qu'une telle communication ne soit pas possible[370]. À cette interrogation et cette crainte, il est répondu dans les travaux préparatoires que le médecin ne pourra transmettre ces données que dans les limites établies par l'article 61 de la loi relative aux assurances[371].

[366] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, amendements, Doc., Ch., 2019-2020, n°0263/008, p. 8 ; J.-M. BINON, *op. cit*., p. 1968.
[367] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, rapport de la deuxième lecture fait au nom de la Commission de l'économie, de la protection des consommateurs et de l'agenda numérique, *Doc*., Ch., 2019-2020, n°0263/009, p. 3.
[368] J.-M. BINON, *op. cit*., p. 1968.
[369] J.-M. BINON, *ibidem*., p. 1967.
[370] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, rapport de la première lecture fait au nom de la Commission de l'économie, de la protection des consommateurs et de l'agenda numérique, *Doc*., Ch., 2019-2020, n°0263/005, p. 10 et 11.
[371] Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, rapport de la deuxième lecture fait au nom de la Commission de l'économie, de la protection des consommateurs et de l'agenda numérique, *Doc*., Ch., 2019-2020, n°0263/009, p. 7.

## §4. L'encadrement juridique des objets connectés dans les assurances en France

Chez nos voisins Français, il n'existe pas de loi semblable à celle du 10 décembre 2020. Il y a toutefois eu une tentative de réglementer l'utilisation, par les assureurs, de données issues d'objets connectés avec le dépôt, le 23 janvier 2019, d'une proposition de loi visant à interdire l'usage des données personnelles collectées par les objets connectés dans le domaine des assurances motivée par le risque de segmentation abusive qu'une telle utilisation pourrait entrainer entre les individus en bonne santé et ceux en mauvaise santé. Cette proposition de loi contient un article unique qui dispose qu' « aucune segmentation ne peut être opérée sur le plan de l'acceptation, de la tarification ou de l'étendue de la garantie sur la base de la condition que le preneur d'un produit répondant aux définitions contenues dans le code des assurances ou du code de la mutualité accepte d'acquérir ou d'utiliser un capteur de santé ni sur la base de l'utilisation de ce capteur de santé par le preneur d'un tel produit. Le traitement de données à caractère personnel récoltées par un capteur de santé, relatives au mode de vie ou à l'état de santé du preneur d'un produit répondant aux définitions contenues dans le code des assurances ou du code de la mutualité est interdit »[372]. Cette proposition de loi n'aboutit toutefois pas, probablement jugée comme étant une interdiction trop absolue eu égard à la marge de manœuvre laissée aux États membres par l'article 9, §4 du RGPD. Il est à noter que la formulation de la proposition de loi française est proche de celle de la loi belge. Déposée le 20 juin 2019, la proposition de loi belge s'est probablement inspirée de la proposition de loi française. Il est donc intéressant de constater que deux propositions de loi à la formulation semblable et s'appuyant sur le même article du RGPD n'ont pas reçu le même sort dans leurs pays respectifs, la proposition de loi belge ayant quant à elle été adoptée. Cela tient probablement au fait, comme nous l'avons vu, que dans la loi belge, le terme d'*interdiction* est remplacé par le terme de *restriction*.

Ainsi, en l'absence d'une réglementation spécifique, seul le RGPD régit l'utilisation de données provenant d'objets connectés dans le domaine des assurances en France[373]. Cette utilisation est dès lors conditionnée au consentement de l'assuré[374]. À cet égard, la CNIL estime que le consentement n'est pas un critère adéquat pour encadrer le traitement par les assureurs de

[372] Proposition de loi n°1603 du 23 janvier 2019 visant à interdire l'usage des données personnelles collectées par les objets connectés dans le domaine des assurances, disponible sur www.assemblee-nationale.fr.
[373] X, « Assurances et objets connectés : l'épineuse question des données personnelles », disponible sur www.selectra.info, mis à jour le 22 juin 2023.
[374] D. COCTEAU-SENN, A. CHARPENTIER et R. BIGOT, *op. cit*., p. 7.

données personnelles issues d'objets connectés, « la divulgation volontaire par certains d'informations personnelles dans des contextes compétitifs comme celui de l'emploi ou de l'assurance oblige tous les autres à divulguer eux aussi des informations du même type sous peine de subir un désavantage compétitif ou de voir leur refus de divulgation interprété – par l'employeur, par l'assureur – comme un indice de « mauvais risque » »[375]. Par ailleurs, le consentement de l'assuré portant sur l'utilisation de l'objet connecté ne signifie pas que ce dernier consente au traitement de toutes les données qui sont collectées par ce biais. Affirmer l'inverse serait contraire à l'exigence de consentement consacrée par le RGPD[376]. Si les contrats d'assurance couplés à un objet connecté viennent à se généraliser, nous pouvons nous interroger sur la réelle effectivité du consentement en tant que critère permettant de réguler le traitement par les assureurs de données personnelles provenant d'objets connectés. En effet, le Code des assurances français dispose que « l'assuré est obligé […] de répondre exactement aux questions posées par l'assureur, notamment dans le formulaire de déclaration du risque par lequel l'assureur l'interroge lors de la conclusion du contrat, sur les circonstances qui sont de nature à faire apprécier par l'assureur les risques qu'il prend en charge »[377]. Par l'usage du terme *notamment* dans l'article, il n'est pas exclu qu'une information que seul un objet connecté peut donner soit un jour considérée comme une circonstance de nature à faire apprécier le risque par l'assureur. Si tel est le cas, le candidat à l'assurance, qui est obligé par la loi de communiquer à l'assureur cette information, se voit contraint d'accepter l'utilisation d'un objet connecté, sous peine de se voir opposer un refus d'assurance[378].

Bien qu'il n'existe pas encore de réglementation spécifique concernant l'utilisation des objets connectés dans le domaine des assurances en France, le législateur français s'est récemment penché sur l'utilisation d'appareils connectés en matière pénale. En effet, le 5 juillet 2023, l'Assemblée nationale adopte en première lecture un projet de loi d'orientation et de programmation du Ministère de la Justice dont l'article 3 prévoit la possibilité d'activer à distance des appareils connectés à l'insu de personnes visées dans certaines enquêtes pénales.

Quant au législateur européen, ce dernier prend également des initiatives touchant aux objets connectés. Ainsi, le 15 septembre 2022, la Commission européenne a adopté la proposition de

[375] CNIL, « Le corps, nouvel objet connecté. Du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde », Cahiers IP n°2, disponible sur www.cnil.fr, mai 2014, p. 53.
[376] D. COCTEAU-SENN, A. CHARPENTIER et R. BIGOT, *op. cit*., p. 7.
[377] Code des assurances, art. L.113-2.
[378] D. COCTEAU-SENN, A. CHARPENTIER et R. BIGOT, *op. cit*., p. 8.

règlement du Parlement européen et du Conseil, le *Cyber Resilience Act*[379]. Ce règlement, actuellement en cours de discussion, établit des normes en matière de cybersécurité pour les produits comportant des éléments numériques, tels que les objets connectés, afin de pallier le vide juridique qui existe dans le domaine[380].

Au sein de cette Section, nous nous sommes penchés sur la particularité des objets connectés dans le traitement des données de santé. Les objets connectés, du fait de leur contemporanéité, ne nous permette certainement pas d'avoir le recul nécessaire pour en comprendre tous les enjeux alors que nous rédigeons ce mémoire. Toutefois, il nous a paru important de donner quelques éléments sur un régime juridique en construction, avec les difficultés que cela emporte d'appréhender un phénomène évoluant bien plus vite que le droit. Par ailleurs, au regard de notre contexte, nous pouvons avoir un aperçu des défis futurs. Nous avons ainsi mis en avant une évolution paradigmatique concernant le droit des assurances, et en particulier la mutualisation des risques et la personnalisation de plus en plus grande des services assurantiels.

[379] Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020, COM (2022) 454 final, 15 septembre 2022.
[380] Conseil de l'Union européenne, « Législation sur la cyberrésilience : les États membres arrêtent une position commune sur les exigences en matière de sécurité concernant les produits numériques », disponible sur www.consilium.europa.eu, 19 juillet 2023.

## Conclusion

Dans le cadre de ce mémoire, nous avons voulu étudier les défis soulevés par la question d'une protection effective des données de santé dans le monde des assurances, à l'aune de l'évolution des nouvelles technologies de l'information et de la communication.

Dans une réflexion scindée en deux, nous avons d'abord remarqué que les données de santé bénéficiaient d'un régime de protection soutenue par rapport à d'autres données personnelles. Le législateur national et, surtout, le législateur européen ont conditionné l'usage et la manipulation de telles données à un consentement explicite et éclairé de la personne concernée. Tout au long de ce mémoire, nous avons toutefois mis en évidence des situations pratiques où le respect de cette exigence était mise à rude épreuve.

Dans cette analyse générale, nous avons également pu voir que les assurances se plaçaient comme les premières garantes de cette protection accrue des données de santé. Elles se sont ainsi présentées comme des actrices à part entière dans l'application du RGPD. Pour autant, du fait de la nature même des contrats d'assurance et du caractère asymétrique de ceux-ci, il est apparu que le rôle des assurances était en réalité ambigu.

Afin d'étudier cette ambiguïté, il nous a paru important, dans le deuxième temps de notre réflexion, de faire état de trois cas juridiques en lien avec la protection des données de santé et les assurances : il s'est agi du cas des détectives privés, des médecins-conseils et des objets connectés. De prime abord assez éloignés, ces cas ont pour particularité de questionner le régime juridique actuel de la protection des données de santé dans les assurances.

Ainsi, le recours aux détectives privés est justifié par une multiplication de la fraude à l'assurance, mais un tel recours doit se faire dans le respect de la vie privée de l'assuré, vie privée qui est un concept englobant, comprenant les données de santé. Législateur et juge ont alors encadré la fonction particulière de détective privé.

Les médecins-conseils œuvrant auprès des assurances ont également la possibilité de manipuler des données de santé. Comme nous l'avons vu, un mille-feuille législatif rend parfois difficile l'appréhension de leur fonction et les patients ne sont pas à l'abri d'une utilisation abusive de leurs données médicales.

Enfin, les objets connectés, qui ne sont certes pas nouveaux mais dont l'usage s'est démultiplié dans notre quotidien, renouvellent la question des modalités de la protection des données de santé. Entre une interdiction pure et simple de leur usage par les assurances dans certains pays européens et une plus grande flexibilité prônée par d'autres, il n'existe aujourd'hui pas de réponse unifiée à ce sujet.

Ces trois cas ont permis par ailleurs d'illustrer ce que l'étude du régime juridique des assurances et de la protection des données de santé avaient pu mettre en évidence, à savoir des sources juridiques plurielles et de différentes natures, voire parfois non existantes. Ces régimes fragmentés sont alors difficiles à appréhender dans leur ensemble mais en même temps, cela illustre d'une certaine souplesse et rend compte du processus de leur construction. Dans l'ensemble, nous avons pu étudier le retard du droit par rapport au développement exponentiel des nouvelles technologies – et surtout celui des objets connectés, sur lesquels nous souhaiterions clore notre réflexion, car ils sont caractérisés par leur transversalité.

Il est vrai que l'importance des objets connectés dans les assurances est à relativiser. Bien que présentant de nombreux avantages pour les assureurs comme vu ci-dessus, les objets connectés mettent les assureurs face à un certain nombre de défis, au premier rang desquels figure la protection de la vie privée de leurs assurés. Les assureurs devront se conformer aux réglementations en matière de protection de la vie privée et s'assurer que les données de leurs assurés sont protégées afin de pallier les réticences de ces derniers de partager leurs données issues d'un objet connecté. Les assureurs devront également faire face à une importante concurrence, notamment de la part des GAFA qui sont des habitués de la collecte massive de données et qui maîtrisent parfaitement le Big Data depuis des années. Aussi, l'intérêt des objets connectés étant de réduire les risques, les assurés pourraient ne plus être convaincus de la nécessité de souscrire une assurance. Les assureurs devront donc se démarquer afin d'apporter une plus-value sur le marché, notamment en développant davantage leur rôle de conseil[381].

Par ailleurs, l'utilisation d'objets connectés dans les assurances de personnes en vue de récolter des données relatives au mode de vie et à la santé des individus est intrinsèquement liée à au développement des objets connectés dans le secteur médical. Il est intéressant de souligner que, comme nous l'observons pour le secteur des assurances, l'utilisation d'objets connectés dans le

[381] G. SCOTTO DI CARLO, « Comment les assureurs peuvent-ils utiliser les objets connectés pour mieux évaluer le risque ? », disponible sur www.bonne-assurance.com, *s.d.*, consulté le 22 juillet 2023, p. 9 à 11.

secteur médical a entrainé un changement de paradigme de la médecine. En effet, en rendant possible au quotidien la surveillance de ses paramètres de santé (*i.e.* le « quantified self »), les objets connectés élargissent l'accès à l'information médicale pour ses utilisateurs, leur permettant de prévenir et de réduire les risques, ainsi que d'obtenir un traitement plus rapidement. Dans ce nouveau paradigme, la focale est donc mise sur les individus sains en vue de leur permettre de maîtriser de manière optimale leur santé. Par ailleurs, l'utilisation d'objets connectés en médecine entraine une modification de la relation médecin-patient en raison des nouvelles données que transmettent les objets connectés. Ainsi, la prise en charge et le suivi du patient s'en voient améliorés[382].

De façon générale, l'analyse des objets connectés dans le droit des assurances en rapport avec la santé apporte également des promesses bienheureuses, en lien avec cette prédictibilité que nous venons de développer : nous nous attendons à une certaine équité, avec une meilleure adaptation aux besoins des preneurs d'assurances. En même temps, cela nous invite aussi à repenser la logique de la responsabilité qui sous-tend nos sociétés européennes. Reposant aujourd'hui sur une logique de la responsabilité collective venant pallier les inégalités sur le plan individuel, un tel modèle pourrait se voir substituer celui de la responsabilité individuelle poussée à l'extrême : si dans un monde utopique et égalitaire cela pourrait se justifier, le risque n'est-il pas l'exacerbation des inégalités sociales dans notre société actuelle ?

[382] Withings Health Institute, « Livre blanc de la santé connectée. Pour entrer dans la médecine 2.0 », disponible sur www.automesure.com, *s.d.*, consulté le 2 août 2023, p. 16 à 42.

# Bibliographie

## Législation

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, *err.*, 29 juin 1961, art. 8.

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, conclue au sein du Conseil de l'Europe le 28 janvier 1981, *S.T.C.E.*, n°108.

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L281, 23 novembre 1995.

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L119, 4 mai 2016, art. 4, 5, 6, 9, 16, 30, 33, 34, 35, 36, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 52, 77.

Directive (UE) 2019/1937 du Parlement européen et du Conseil sur la protection des personnes qui signalent des violations du droit de l'Union, *J.O.U.E.*, L305, 26 novembre 2019.

Const., art. 22.

C. civ., art. 1349 et 1353.

Code des assurances, art. L.113-2.

Loi du 17 juin 1991 portant approbation de la convention relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981, *M.B.*, 30 décembre 1993.

Loi du 19 juillet 1991 organisation la profession de détective privé, *M.B.*, 2 octobre 1991, art. 1, 2, 3, 7, 8, 9, 10, 11.

Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.

Loi du 11 avril 1995 visant à instituer « la charte » de l'assuré social, *M.B.*, 6 septembre 1995.
Loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, *M.B.*, 27 août 1994 .

Loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 février 1999.

Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 20 décembre 2002, art. 2, 3.

Loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, art. 5, 46/1, 46/2, 46/3, 58, 61.

Loi coordonnée du 10 mai 2015 relative à l'exercice des professions des soins de santé, *M.B.*, 18 juin 2015, art. 2.

Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, art. 7, 23, 32, 34, 36, 43, 44, 95, 99, 100, 102, 108.

Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, art. 9.

Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *M.B.*, 10 septembre 2018, art. 2.

Loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé, *M.B.*, 14 mai 2019, art. 3, 34, 36, 37, 38, 39, 40.

Loi du 10 décembre 2020 modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir dans le domaine de l'assurance maladie et de l'assurance individuelle sur la vie une restriction de traitement des données à caractère personnel concernant le mode de vie ou la santé issues des objets connectés, *M.B.*, 15 janvier 2021.

Loi du 28 novembre 2022 sur la protection des personnes qui signalent des violations au droit de l'Union ou au droit national constatées au sein d'une entité juridique du secteur privé, *M.B.*, 15 décembre 2022.

Loi du 14 mars 2023 relative à l'institution et à l'organisation de l'Agence des données de (soins de) santé, *M.B.*, 3 avril 2023, art. 2, 4.

Arrêté royal 35 du 20 juillet 1967 portant le statut et le barème des médecins-conseil chargés d'assurer auprès des organismes assureur le contrôle médical de l'incapacité primaire et des prestations de santé en vertu de la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, *M.B.*, 29 juillet 1967.
Code de déontologie médicale, art. 43.

Avis de la Commission des Communautés européennes concernant la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, COM (1995), 375 final, 18 juillet 1995.

Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, COM (2021) 206 final, 21 avril 2021.

Proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020, COM (2022) 454 final, 15 septembre 2022.

Proposition de directive du Parlement européen et du Conseil relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle (directive sur la responsabilité en matière d'IA), COM (2022) 496 final, 28 septembre 2022.

Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, exposé des motifs, *Doc., Ch*., 1990-1991, n°1610/1.

Projet de loi organisant la profession de détective privé, discussion des articles, *Doc. Sén*., 1990-1991, n°1259/2.

Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, rapport fait au nom de la commission de la justice, *Doc., Ch*., 1991-1992, n°413/12.

Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, rapport fait au nom de la commission de la justice, *Doc., Sén*., 1992-1993, n°445/2.

Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, exposé des motifs, *Doc., Ch*., 1997-1998, n°1566/1.

Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, rapport fait au nom de la commission de la justice, *Doc., Ch*., 1998-1999, n°1566/10.

Projet de loi relatif à la qualité de la pratique des soins de santé, commentaire des articles, *Doc., Ch*., 2018-2019, n°3441/001.

Proposition de loi n°1603 du 23 janvier 2019 visant à interdire l'usage des données personnelles collectées par les objets connectés dans le domaine des assurances, disponible sur www.assemblee-nationale.fr.

Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, *Doc*., Ch., 2019-2020, n°0263/001.

Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, amendement, *Doc*., Ch., 2019-2020, n°0263/004.

Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, rapport de la première lecture fait au nom de la Commission de l'économie, de la protection des consommateurs et de l'agenda numérique, *Doc*., Ch., 2019-2020, n°0263/005.

Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, amendements, Doc., Ch., 2019-2020, n°0263/008.

Proposition de loi modifiant la loi du 4 avril 2014 relative aux assurances en vue d'établir une restriction d'usage des données personnelles issues des objets connectés dans le domaine de l'assurance maladie et de l'assurance sur la vie, rapport de la deuxième lecture fait au nom de la Commission de l'économie, de la protection des consommateurs et de l'agenda numérique, *Doc*., Ch., 2019-2020, n°0263/009.

Projet de loi relatif à l'institution et à l'organisation de l'Agence des données de (soins de) santé, *Doc., Ch*., 2022-2023, n°3065/001.

Projet de loi relatif à l'institution et à l'organisation de l'Agence des données de (soins de) santé, rapport de la première lecture fait au nom de la commission de la Santé et de l'Égalité des chances, *Doc., Ch*., 2022-2023, n° 3065/004.

**Doctrine**

AMANKWAH, J., « In het licht van de AVG : het verwerken van bijzondere categorieën van persoonsgegevens in de verzekeringssector », *T.B.H.*, 2019/2, p. 245 à 254.

BENHATTA, N. et CHAMBA, H., *Appliquer le RGPD dans l'assurance*, 2e éd., Paris, L'Argus de l'assurance Éditions, 2022.

BINON, J.-M., « Assurances de personnes et protection des données personnelles : un mariage tumultueux à l'ombre du RGPD », *R.D.C.*, 2021/9, p. 1949 à 1971.

BOULANGER, M.-H., « Quelques remarques sur les autorités indépendantes de protection des données dans l'ordre juridique européen », *Le règlement général sur la protection des données (RGPD/GPDR) – Analyse approfondie*, C. de Terwangne et K. Rosier (dir.), Collection du CRIDS, Bruxelles, Larcier, 2018, p. 473 à 491.

CLUYDTS, S., « Jurisprudence Antigone. Application par les juridictions du travail et conséquences de l'arrêt du 14 juin 2021 de la Cour de cassation », *Licenciements & Démission*, n°1, p. 1 à 12.

DAUTIEU, T., « La commission nationale de l'informatique et des libertés, régulateur des données de santé », *Les tribunes de la santé*, vol. 1, n°58, 2018, p. 47 à 52.

DEGRAVE, E., « L'autorité de contrôle », *Le règlement général sur la protection des données (RGPD/GPDR) – Analyse approfondie*, C. de Terwangne et K. Rosier (dir.), Collection du CRIDS, Bruxelles, Larcier, 2018, p. 593 à 611.

DEGRAVE, E., « Le R.G.P.D., les lois belges et le secteur public – Les traitements de données dans l'administration en réseaux et l'Autorité de protection des données », *Le règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, H. Jacquemin (dir.), Commission Université – Palais – Université de Liège, Liège, Anthemis, 2020, vol. 195, p. 281 à 317.

DEHARENG, E., « La question de la licéité des traitements de données personnelles dans le secteur de l'Assurance, ou quelles bases juridiques pour justifier les traitements de données personnelles ? », *Bull. ass*., 2022/1, n°418, p. 4 à 24.

DE TERWANGNE, C., « Présentation générale du R.G.P.D. et des lois belges relatives à la protection des données », *Le règlement général sur la protection des données (R.G.P.D./G.D.P.R.) : premières applications et analyse sectorielle*, H. Jacquemin (dir.), Commission Université – Palais – Université de Liège, Liège, Anthemis, 2020, vol. 195, p. 7 à 58.

DOUVILLE, T., « Les dangers de la collecte des données de santé par les tiers intéressés (GAFAM, assureurs…) », *Journal de Droit de la Santé et de l'Assurance Maladie*, 2018, n°20, p. 12 à 16.

FIEVET, C., GERARD, L., GILLARD, N., KNOCKAERT, M., MICHEL, A., MONT, J., ROSIER, K., TOMBAL, T. et VANRECK, O., « Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information », *R.D.T.I*., 2017, n°68-69, p. 94 à 163.

FRUY, G., « Une santé déconnectée des assureurs », *Les pages*, n°93, 2020.

GILSON, S. et MENIER, C., « Les conditions d'admissibilité de la preuve par détective privé », obs. sous. Mons (22e ch.), 14 janvier 2020, *For. Ass*, n° 211, 2021, p. 29 à 41.

HOSTAUX, S., *Le droit de l'assurance soins de santé indemnités*, 1ère éd., Bruxelles, Larcier, 2009.

JACQUEMIN, H. et VAN GYSEGHEM, J.-M., « Le big data en matière d'assurances à l'épreuve du RGPD », *Bull. ass*., 2017, n°22, p. 233 à 260.

LEDUC, C., « La preuve d'une fraude à l'assurance : comment mener au mieux l'enquête ? », *Bull. ass*., 2018/1, n°402, p. 4 à 42.

LEONARD, T. et POULLET, Y., « La protection des données à caractère personnel en pleine (r)évolution – La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995 », *J.T.*, n°20, 1999, p. 377 à 396.

LUTTE, I., « L'accès aux données de santé. À propos du dossier médical établi par le médecin-conseil d'une compagnie d'assurance », *Rev. dr. santé*, n°3, 2020, p. 259 à 265.

LUTTE, I., « Le dossier médical et les données de santé sous le prisme de la « loi qualité », *Revue belge du dommage corporel et de médecine légale*, 2021/2, p. 51 à 65.

MOUGENOT, D., « La preuve irrégulière : quand Antigone ouvre la boîte de Pandore. Commentaire de l'arrêt *Lee Davies* rendu par la Cour européenne des droits de l'homme le 28 juillet 2009 », *Chr. D.S.*, 2010, n°6, p. 289 à 292.

MOUGENOT, D., « Humphrey Bogart au XXIe siècle : la preuve par production d'un rapport de détective privé », note sous C. trav. Liège, 15 décembre 2008, *Rev. rég. dr.*, p. 236 à 260.

PARIS, C., *Manuel de droit des assurances*, 1ère éd., Bruxelles, Larcier, 2021.

REGOUT, G., « Assurances : le profilage et autres traitements automatisés de données à caractère personnel, à l'épreuve du nouveau règlement général sur la protection des données », *Bull. ass.*, 2018/3, n°404, p. 307 à 318.

REUSENS, I., « De quelques modes de preuve en droit de la responsabilité à la lumière de la protection de la vie privée », *Droit de la responsabilité*, I. Reusens (dir.), 1ère éd., Bruxelles, Larcier, 2015, p. 22 à 52.

ROLAND, N., « Comment (ré)concilier le rapport d'un détective privé avec la réglementation vie privée ? », *DPO news*, n°12, p. 15 à 17.

SANTANTONIO, O., « Exposé introductif du règlement général sur la protection des données », *Bull. ass.*, 2017, n°22, p. 17 à 38.

STROOBANTS, N., « Het gebruik van persoonsgegevens inzake levensstijl of gezondheid verzameld door met het internet verbonden apparaten in individuele levensverzekeringen en ziekteverzekeringen: het segmentatiebeleid van private verzekeraars verder aan bander gelegd », *R.D.C.*, 2021/9, p. 1930 à 1948.

THELISSON, E., « La portée du caractère extraterritorial du Règlement général sur la protection des données », *R.I.D.E.*, 2019, t. XXXIII, n°4, p. 487 à 541.

VAN GOSSUM, L., note sous C. trav. Bruxelles, 18 mars 2002, *Bull. Ass*., 2002, p. 645.

VAN GYSEGHEM, J.-M., « Les catégories particulières de données à caractère personnel », *Le règlement général sur la protection des données (RGPD/GPDR) – Analyse approfondie*, C. de Terwangne et K. Rosier (dir.), Collection du CRIDS, Bruxelles, Larcier, 2018, p. 255 à 284.

VAN OLDENEEL, C.-A., « Protection des données – Amende de 50.000€ pour une entreprise d'assurances », *Bull. ass*., 2020/3, n°412, p. 319 et 320.

VINCINEAU, M., « Assurances et vie privée. Du vide légal à l'illicite », *R.B.D.I.*, 1994/2, p. 480 à 532.

VITALIS, A., *Informatique, pouvoir et libertés*, 2e éd., Paris, Economica, 1988.

**Jurisprudence**

Cour eur. D.H., arrêt *Elvir Mehmedovic et Eldina Mehmedovic c. Suisse*, 17 janvier 2019.

Cour eur. D.H., arrêt *Verlière c. Suisse*, 28 juin 2001.

C.J., arrêt *Land Hessen*, 9 juillet 2020, C-272/19, EU:C:2020:535.

C.J., arrêt *Fashion ID*, 29 juillet 2019, C-40/17, EU:C:2019:629.

C.J., arrêt *Jehovan todistajat*, 10 juillet 2018, C-25/17, EU:C:2018:551.

C.J., arrêt *Wirtschaftsakademie Schleswig Holstein*, 5 juin 2018, C-210/16, EU:C:2018:388.

C.J., arrêt *Tele2 Sverige*, 21 décembre 2016, aff. jointes C-203/15 et C-698/15, EU:C:2016:970.

C.J., *arrêt Schrems*, 6 octobre 2015, C-362/14, EU:C:2015:650.

C.J., arrêt *Digital Rights Ireland e.a.*, 8 avril 2014, aff. jointes C293/12 et C-594/12, EU:C:2014:238.

C.J., arrêt *Commission c. Hongrie*, 8 avril 2014, C-288/12, EU:C:2014:237.

C.J., arrêt *République d'Autriche c. Commission*, 16 octobre 2012, C-614/10, EU:C:2012:605.

C.J., arrêt *Volker und Markus Schecke et Eifert*, 9 novembre 2010, aff. jointes C-92/09 et C-93/09, EU:C:2010:662.

C.J., arrêt *République fédérale d'Allemagne c. Commission*, 9 novembre 2010, C-518/07, EU:C:2010:125.

C.J.C.E., arrêt *Lindqvist*, 6 novembre 2003, C-101/01, EU:C:2003:596.

C.C., 22 septembre 2022, n°110/2022.

C.C., 27 juillet 2011, n°139/2011.

C.C., 22 décembre 2010, *J.L.M.B.*, 2011, p. 298.

Cass. (1re civ.), 17 mars 2016, n°15-11.412, disponible sur www.legifrance.gouv.fr.

Cass. (1re civ.), 25 février 2016, n°15-12.403, disponible sur www.legifrance.gouv.fr.

Cass. (1re civ.), 31 octobre 2012, n°11-17.476, disponible sur www.legifrance.gouv.fr.

Cass., 10 mars 2008, *J.L.M.B.*, 2009, p. 580.

Cass., 2 mars 2005, *J.T.*, 2005, p. 211.

Cass., 14 octobre 2003, R.G. n°P.03.0762.N., disponible sur www.juridat.be.

Cass., 10 mai 1965, *Pas.*, 1965, p. 952.

Cass., 15 février 1965, *Pas.*, 1965, p. 601.

Cass., 29 octobre 1962, *Pas.*, 1963, p. 272.

Cass., 13 octobre 1952, *Pas.*, 1953, p. 52.

Cass., 2 septembre 1948, *Pas.*, 1948, p. 488.

Cass., 24 mai 1948, *Pas.*, 1948, p. 334.

Cass., 6 mars 1944, *Pas.*, 1944, p. 237.

Cass., 3 février 1941, *Pas.*, 1941, p. 30.

Cass., 4 mars 1929, *Pas*., 1929, p. 118.

Cass., 12 mars 1923, *Pas*., 1923, p. 233.

Mons (22e ch.), 16 juin 2020, *Bull. ass*., liv. 3, p. 369.

Mons (22e ch.), 14 janvier 2020, *For. Ass*., n°211, 2021, p. 41.

Mons (22e ch.), 7 janvier 2020, *For. Ass*., n°211, 2021, p. 41.

Mons (22e ch.), 4 décembre 2018, *R.G.A.R*., 2019/2, p. 15551.

C. trav. Bruxelles (6e ch.), 9 juin 2017, *For. Ass*., 2018, p. 95.

C. trav. Bruxelles (5e ch.), 18 mai 2015, n° 2014/AB/996.

C. trav. Mons, 4 novembre 2013, R.G. n°2011/AM/397, disponible sur www.juridat.be.

C. trav. Liège, 15 décembre 2008, *R.R.D*., 2008, n°127, p. 251.

C. trav. Mons, 22 mai 2007, *R.D.T.I*., 2008, p. 239.

C. trav. Anvers, 1er octobre 2002, *R.W*., 2002-2003, p. 298.

Civ. fr. Bruxelles (87e ch.), 11 janvier 2021, *J.T*., 2021, p. 333.

Civ. Charleroi, 1er octobre 2020, R.G., n°14/3360/A, *inédit*.

Comm. Bruxelles (cess.), 9 mars 2018, A/17/01046.

Comm. Bruxelles (cess.), 9 mars 2018, A/17/01140.

Comm. Bruxelles (cess.), 9 mars 2018, A/17/01141.

Trib. trav. Hainaut, div. Tournai, 19 janvier 2018, R.G. n°14/504/A, disponible sur www.terralaboris.be.

Trib. trav. Liège, 23 novembre 2017, R.G. n°16/6623/A, disponible sur www.terralaboris.be.

Trib. trav. Charleroi (1ère ch.), 16 juin 2010, *Bull. Ass*., 2010/3, p. 292.

Civ. Anvers, 7 mars 2007, R.W., 2008-2009, p. 332.

Comm. Bruxelles (cess.), 16 juin 2003, *Test-Achats/DKV Belgium*, *R.D.C*., 2003, p. 901.

Chambre contentieuse de l'Autorité de protection des données, 19 juillet 2022, 115/2022, disponible sur www.autoriteprotectiondonnees.be.

Chambre contentieuse de l'Autorité de protection des données, 9 juillet 2021, 76/2021, disponible sur www.autoriteprotectiondonnees.be.

Chambre contentieuse de l'Autorité de protection des données, 23 décembre 2020, 81/2020, disponible sur www.autoriteprotectiondonnees.be.

Chambre contentieuse de l'Autorité de protection des données, 14 mai 2020, 24/2020, disponible sur www.autoriteprotectiondonnees.be.

Chambre contentieuse de l'Autorité de protection des données, 6 mai 2021, 57/202, disponible sur www.autoriteprotectiondonnees.be.

**Sources diverses**

AFP, « Le Parlement européen veut mieux encadrer ChatGPT », disponible sur www.lesoir.be, 11 mai 2023.

AFP, « Les institutions européennes veulent interdire TikTok à leurs personnels pour « protéger » leurs données », disponible sur www.rtl.be, 23 février 2022.

Allianz, « Déclaration sur la protection des données personnelles », disponible sur www.allianz.be, novembre 2021.

ALLO, M., « L'Union européenne adopte un nouveau cadre légal pour le transfert de données vers les États-Unis », disponible sur www.rtbf.be, 10 juillet 2023.

Assuralia, « La protection de vos données de santé chez l'assureur », disponible sur www.abcassurance.be.

Assuralia, « Les assureurs unissent leurs efforts dans la lutte contre la fraude. Création d'une banque de données sinistres : une primeur pour le secteur de l'assurance », disponible sur www.assuralia.be, 25 janvier 2021.

Assurdeal, « Les courtiers belges ont aussi à se mettre en conformité #GDPR (#RGPD en France) », disponible sur www.assurdeal.media, 9 mai 2018.

Autorité de protection des données, « La Chambre contentieuse dans les grandes lignes », disponible sur www.autoriteprotectiondonnees.be.

Autorité de protection des données, « Avis concernant un avant-projet de loi modifiant la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (AH-2022-0020), disponible sur www.autoriteprotectiondonnees.be, 25 février 2022.

Autorité de protection des données, « Lettre aux parlements et gouvernements belges », disponible sur www.autoriteprotectiondonnees.be, 2 février 2021.

Autorité de protection des données, « Traitement de données provenant de dossiers de patients – Demande d'avis de la Ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration », disponible sur www.autoriteprotectiondonnees.be, DOS-2019-04611.

Avis de la Commission des assurances sur l'avant-projet de loi relatif au traitement des données à caractère personnel concernant la santé, Doc/C2021/3, 20 décembre 2021.

Avis de la Commission des assurances concernant le traitement des données relatives à la santé dans le cadre du règlement UE 2016/679 (règlement général sur la protection des données), Doc/C2019/1, 16 juillet 2019.

BELGA, « La réforme de l'Autorité de Protection des Données repart pour la quatrième fois au Conseil d'État », 1er juin 2023.

BELGA, « Vie privée sous tension – Le projet de loi réformant l'APD renvoyé une nouvelle fois au Conseil d'État », disponible sur www.lalibre.be, 30 mars 2023.

BELGA, « L'Absym demande des éclaircissements sur la plateforme en ligne Helena », disponible sur www.rtbf.be, 28 octobre 2021.

BELGA, « Plainte à l'APD au sujet d'Helena : Helena ne représente pas une menace, selon mypension.be », disponible sur www.numerikare.be, 27 octobre 2021.

BELGA, « Protection des données de santé dans l'app Helena : une plainte déposée à l'Autorité de protection des données », disponible sur www.rtbf.be, 27 octobre 2021.

BELGA, « RGPD : la Commission européenne ouvrira une procédure d'infraction contre la Belgique », disponible sur www.rtbf.be, 9 juin 2021.

BONNIER, C., « La CNIL surveille le secteur de l'assurance », disponible sur www.actu-juridique.fr, 12 mai 2022.

BOUCHER, P., « « Safari » ou la chasse aux Français », disponible sur www.lemonde.fr, 21 mars 1974.

BOUNEMOURA, H., « Facebook : Tout comprendre à la fuite de données qui concerne 533 millions d'utilisateurs », disponible sur www.20minutes.fr, 7 avril 2021.

BURGESS, M., « What is GDPR ? The summary guide to GDPR compliance in the UK », disponible sur www.wired.co.uk, 24 mars 2020.
Cellule stratégique de la Ministre des Affaires sociales et de la Santé publique, « Pacte d'avenir avec les organismes assureurs », disponible sur www.ocm-cdz.be, septembre 2016.

Chambre des salariés Luxembourg, « avis III/29/2020 relatif au projet de loi relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances », disponible sur www.csl.lu, 28 mai 2020.

CNIL, « Les fiches pratiques pour le secteur de l'assurance », disponible www.cnil.fr.

CNIL, « Pack de conformité : véhicules connectés et données personnelles », disponible sur www.cnil.fr.

CNIL, « Rapport annuel 2021 », disponible sur www.cnil.fr.

CNIL, « La qualification des acteurs du secteur de l'assurance au regard du RGPD », disponible sur www.cnil.fr, 16 juillet 2021.

CNIL, « Les grands traitements du secteur de l'assurance et leurs bases légales », disponible sur www.cnil.fr, 16 juillet 2021.

CNIL, « Les durées de conservation des données du secteur de l'assurance », disponible sur www.cnil.fr, 16 juillet 2021.

CNIL, « Le principe de minimisation et les traitements du NIR et des données de santé dans le secteur de l'assurance », disponible sur www.cnil.fr, 16 juillet 2021.

CNIL, « Droit des personnes et profilage : les spécificités du secteur de l'assurance », disponible sur www.cnil.fr, 16 juillet 2021.

CNIL, « Adopter les six bons réflexes », disponible sur www.cnil.fr, 18 septembre 2019.

CNIL, « Le corps, nouvel objet connecté. Du quantified self à la M-Santé : les nouveaux territoires de la mise en données du monde », Cahiers IP n°2, disponible sur www.cnil.fr, mai 2014.

COCTEAU-SENN, D., CHARPENTIER, A. et BIGOT, R., « La protection des données personnelles en assurance – dialogue du juriste avec l'actuaire », disponible sur www.f-origin.hypotheses.org.

Commission européenne, « Protection des données : la Commission adopte de nouvelles règles pour renforcer l'application du RGPD dans les situations transfrontalières », communiqué de presse, disponible sur www.ec.europa.eu, 4 juillet 2023.

Commission européenne, « De nouvelles règles en matière de responsabilité applicables aux produits et à l'IA pour protéger les consommateurs et favoriser l'innovation », disponible sur www.france.representation.ec.europa.eu, 28 septembre 2022.

Commission nationale pour la protection des données du Grand-Duché de Luxembourg, « avis de la Commission nationale pour la protection des données relatif au projet de la loi n°7511 relative au traitement de données concernant la santé en matière d'assurance et de réassurance et portant modification de la loi modifiée du 7 décembre 2015 sur le secteur des assurances », disponible sur www.cnpd.public.lu, 27 janvier 2020.

Commission nationale pour la protection des données du Grand-Duché de Luxembourg, « Documentation et responsabilisation », disponible sur www.cdnp.public.lu, 19 juin 2018.

Comité européen de la protection des données, « Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD », disponible sur www.edpb.europa.eu, 7 juillet 2021.

Comité sectoriel de la sécurité sociale et de la santé (section « santé )», « Recommandation n°17/01 du 16 mai 2017 relative à l'incompatibilité entre le rôle de prestataire de soins ayant une relation thérapeutique et le rôle de médecin-conseil, contrôleur ou expert à la demande d'un tiers à l'égard du même patient », disponible sur www.ehealth.fgov.be, 16 mai 2017.

Conseil de l'Union européenne, « Législation sur la cyberrésilience : les États membres arrêtent une position commune sur les exigences en matière de sécurité concernant les produits numériques », disponible sur www.consilium.europa.eu, 19 juillet 2023.

Conseil national de l'Ordre des médecins, « Accès aux données médicales d'une personne par le médecin chargé d'évaluer son état de santé », disponible sur www.ordomedic.be, 15 février 2020.

Conseil national de l'Ordre des médecins, « force obligatoire du Code de déontologie médicale », disponible sur www.ordomedic.be, 16 juin 2018.

Cour eur. D.H., « Guide sur l'article 8 de la Convention – Droit au respect de la vie privée et familiale, du domicile et de la correspondance, disponible sur www.echr.coe.int, mis à jour au 31 août 2022.

Courrier de l'Observatoire des maladies chroniques au Président/à la Présidente du comité SECM *et al*., le 20 août 2018 à Bruxelles, disponible sur www.inami.fgov.be.

CRENIER, L. et R. RADERMECKER, R., « Abandon de l'avant-projet Dermagne ! », disponible sur www.diabete.be, 25 janvier 2022.

DASINIERES, L., « Protection des données médicales, discrimination aux soins : les risques de Mon Espace Santé », disponible sur www.numerama.com, 7 janvier 2022.

DEGRAVE, E., « La compétence d'avis de l'Autorité de protection des données : une aide précieuse dans l'élaboration des normes sur les données à caractère personnel et la vie privée », disponible sur www.justice-en-ligne.be, 10 décembre 2021.

DEGRAVE, E., « L'Autorité de protection des données, un nouveau chien de garde de la vie privée des citoyens », disponible sur www.justice-en-ligne.be, 8 janvier 2020.

DE HALLEUX, F., « Les détectives privés ne peuvent pas tout faire : la ministre Verlinden va les recadrer ! », disponible sur www.sudinfo.be, 19 décembre 2022.

DELVAUX, B. et LALOUX, P., « Charlotte Dereppe : « On était à l'APD pour se taire, pas pour protéger la vie privée » », disponible sur www.lesoir.be, 31 octobre 2022.

DELEPIERRE, F., « Le vrai ou faux : les entreprises publiques font-elles appel à des détectives privés ? », disponible sur www.lesoir.be, 25 décembre 2022.

DEL SOL, M., « Enjeux juridiques des objets connectés en matière d'assurance santé. Réflexions à partir et au-delà du cadre français », disponible sur www.shs.hal.science, 12 juillet 2018.

DERVAL, T., « Les assureurs peuvent-ils utiliser les données issues d'objets connectés ? », disponible sur www.lecho.be, 10 mars 2021.

DEVILLARD, A., « Sous Giscard, la création de la Cil après un "SAFARI" », disponible sur www.sciencesetavenir.fr, 4 décembre 2020.

ETech, « Quand les objets connectés ont besoin d'intelligence artificielle », disponible sur www.etechconsulting-mg.com, 30 septembre 2021.

Ethias, « Traitement de données relatives à la santé et/ou autres donnés sensibles », disponible sur www.ethias.be.

EWALD, F., « Assurance, prévention, prédiction… dans l'univers du Big Data », Rapport pour l'Institut Montparnasse, disponible sur www.institut-montparnasse.eu, octobre 2012.
France assureurs, « Guide actualisant le Pack de conformité Assurance », disponible sur www.franceassureurs.fr.

France assureurs, « Traitement des données à caractère personnel : guide d'actualisation du Pack de conformité assurance », disponible sur www.franceassureurs.fr, 15 juillet 2021.

GALLE, C., « Verzekeringsartsen kunnen meekijken in uw medisch dossier », disponible sur www.demorgen.be, 23 janvier 2020.

Groupe de travail « article 29 », « Lignes directrices sur le consentement au sens du règlement 2016/679 », disponible sur www.cnil.fr, 10 avril 2018.

Groupe de travail « article 29 » sur la protection des données, « Document de travail sur le traitement des données relative à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME) », WP 131, disponible sur www.ec.europa.eu, 15 février 2007.

IMEC, « ehealthmonitor 2019 – Résumé », disponible sur www.gcm.rmnet.be.

INAMI, « IV. Directives aux médecins conseil pour l'organisation du contrôle et de l'évaluation de l'incapacité de travail », disponible sur www.inami.fgov.be, 2015/3.

Insurance Europe, « Insurance fraud : not a victimless crime », disponible sur www.insuranceeurope.eu, novembre 2019.

Insurance Europe, « Insurers highlight challenges of applying GDPR », disponible sur www.insuranceeurope.eu, 11 avril 2019.

Insurance Europe, « Insurance Europe comments on consent », disponible sur www.insuranceeurope.eu, 17 juin 2017.

JANSSEN, B. et VAN HECKE, M., « Données médicales en ligne : comment les gérer vous-même ? », disponible sur www.test-achats.be, juin/juillet 2022.

KHELOUFI, M., « Entrée en vigueur du règlement général sur la protection des données : le changement dans la continuité », disponible sur www.revue-jade.eu, 30 octobre 2019.

LALOUX, P., « Critiqué, torpillé, saboté… le projet de loi APD de Mathieu Michel va une nouvelle fois se faire recaler », disponible sur www.lesoir.be, 2 février 2023.

LALOUX, P., « Vie privée : la Belgique une nouvelle fois mise en demeure », disponible sur www.lesoir.be, 6 janvier 2023.

LALOUX, P., « Données de santé : la Cour constitutionnelle détricote le CSI de Frank Robben », disponible sur www.lesoir.be, 22 septembre 2022.

LALOUX, P., « Didier Reynders : « La démission de Frank Robben n'efface pas tous les risques de non-indépendance de l'APD » », disponible sur www.lesoir.be, 8 février 2022.

LALOUX, P., « De justesse, Frank Robben démissionne de son poste à l'Autorité de protection des données », disponible sur www.lesoir.be, 7 février 2022.

LALOUX, P., « Les assureurs veulent accéder à certaines données de santé sans consentement », disponible sur www.lesoir.be, 21 janvier 2022.

LALOUX, P., « Pourquoi le problème de non-indépendance de l'APD est loin d'être réglé », disponible sur www.lesoir.be, 14 janvier 2022.

LALOUX, P., « Alexandra Jaspar démissionne de l'APD : « le système est toxique » », disponible sur www.lesoir.be, 8 décembre 2021.

LALOUX, P., « « Helena « ne représente pas une menace pour vos données de pension. » Vraiment ? », disponible sur www.lesoir.be, 27 octobre 2021.

LALOUX, P., « Vie privée : Helena devrait prévenir tous ses patients d'une potentielle violation de leurs données de santé », disponible sur www.lesoir.be, 27 octobre 2021.

LALOUX, P., « Comment Frank Robben a ouvert une brèche dans l'accès à nos données santé et pension », disponible sur www.lesoir.be, 26 octobre 2021.

LALOUX, P., « Vie privée : le CSI, gestionnaire de données de santé en (tout) petit comité », disponible sur www.lesoir.be, 5 mai 2021.

LAMBERTS, P., « Protection des données personnelles : la Belgique poursuivie par la Commission ! », disponible sur www.philippelamberts.eu, 9 juin 2021.

LIMOGE, F., « John Hancock, l'assureur américain qui traque la bonne santé de ses assurés », disponible sur www.argusdelassurance.com, 24 septembre 2018.

LE PRIOL, M., « Twitter : fuite de données personnelles d'une ampleur inédite pour la plateforme », disponible sur www.la-croix.com, 6 janvier 2023.

LORD, N., « What is the Data Protection Directive ? The Predecessor to the GDPR », disponible sur www.digitalguardian.com, 28 décembre 2022.

MARTIN, A., « Les objets connectés et la conso de données s'envolent », disponible sur www.lecho.be, 9 juin 2022.

Parlement européen, « Loi sur l'IA de l'UE : première réglementation de l'intelligence artificielle », disponible sur www.europarl.europa.eu, 9 juin 2023.

Parlement européen, « Le droit au respect de la vie privée : les défis digitaux, une perspective de droit comparé – Belgique», disponible sur www.europarl.europa.eu, octobre 2018.

PEROCHEAU, J., « Connectes : quels enjeux pour l'assurance ? », disponible sur www.insurancespeaker-wavestone.com, 14 octobre 2019.

PM, « Triste première : un médecin hospitalier consulte abusivement un dossier patient (RSW) », disponible sur www.lespecialiste.be, 8 avril 2019.

RAGOT, J., « TikTok : l'Union européenne lance plusieurs enquêtes sur l'usage des données personnelles par la Chine », disponible sur www.bfmtv.com, 23 novembre 2022.

REDON, M., *L'assurance santé privée à l'épreuve des objets connectés*, Thèse, Université de Rennes 1, disponible sur www.theses.hal.science, 2021.

ROLDAN PEREZ, J., « Un médecin a consulté les dossiers médicaux en ligne de Claire, sans autorisation : « Il est remonté jusqu'en 2003 et il a tout pris » », disponible sur www.rtl.be, 9 avril 2019.

ROSSOW, A., « The Birth of GDPR : What Is It And What You Need To Know », disponible sur www.forbes.com, 25 mai 2018.

SCOTTO DI CARLO, G., « Comment les assureurs peuvent-ils utiliser les objets connectés pour mieux évaluer le risque ? », disponible sur www.bonne-assurance.com, *s.d.*, consulté le 22 juillet 2023.

Sénat français, « Le contexte : l'examen du projet de loi relatif à l'informatique et aux libertés », disponible sur www.senat.fr.

SPF Chancellerie du Premier Ministre – Direction générale Communication externe, « Renforcement de l'indépendance et du fonction de l'Autorité de protection des données – Deuxième lecture », disponible sur www.news.belgium.be, 24 juin 2022.

SPERONI, J., « Fraude à l'assurance : le monde rêvé de la Cour de cassation », disponible sur www.argusdelassurance.com, 7 juillet 2016.

TANGENS, R., « 40 Years of German Privacy Movement », disponible sur www.digitalcourage.de, 17 décembre 2021.

Test-Achats, « Nos données privées de santé sont-elles suffisamment protégées ? », disponible sur www.test-achats.be, 10 novembre 2021.

Test-Achats, « Applications nutrition & santé : protégez vos données privées », disponible sur www.test-achats.be, 23 janvier 2020.

TORREANI, H., « La fraude à l'assurance a doublé en 2022 ! », disponible sur www.lelynx.fr, 30 juin 2022.

V. D., « Détectives privés en assurance », disponible sur www.compareil.fr, 31 août 2021.

VAN DER VEN, M., « 42 pour cent des Belges partagent des données professionnelles avec ChatGPT », disponible sur www.datanews.levif.be, 25 juillet 2023.

VAN REETH, C., « Un médecin consulte les données médicales d'un ex-patient sans autorisation : un incident qui pose question », disponible sur www.lesoir.be, 8 avril 2019.

WERY, E., « IA et données de santé : que prévoit le futur règlement européen ? », disponible sur www.droit-technologie.org, 20 avril 2023.

Withings Health Institute, « Livre blanc de la santé connectée. Pour entrer dans la médecine 2.0 », *s.d.*, consulté le 2 août 2023, disponible sur www.automesure.com.

X, « Pay how you drive », disponible sur www.compare-assurance.be, *s.d.*, consulté le 23 juillet 2023.

X, « Assurances et objets connectés : l'épineuse question des données personnelles », disponible sur www.selectra.info, mis à jour le 22 juin 2023.

X, « Combien pèse le marché des objets connectés en France ? », disponible sur www.boursorama.com, 3 juillet 2022.

X, « Santé : les objets connectés sous la loupe des assureurs », disponible sur www.lesechos.fr, 29 août 2017.

X, « L'impact du RGPD dans le secteur de l'assurance », disponible sur www.donnees-rgpd.fr, 19 décembre 2019.

X, « L'Internet des objets : De nouvelles perspectives pour les assureurs », disponible sur www.headmind.com, 20 mars 2019.

**Tables des matières**

**LOUVAIN-LA-NEUVE** | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/drt**