

TITRE 5

Les catégories particulières de données à caractère personnel¹

Jean-Marc Van GYSEGHEM^{2,3}

Introduction

1. L'on doit aborder cette catégorie de données avec, à l'esprit, le fait qu'on leur réserve une protection plus élevée que celle visée à l'article 6 du RGPD à cause des risques accrus de porter préjudice aux individus sur la base du traitement de ces données. C'est principalement le risque de discriminations illégitimes ou arbitraires qui est lié à ces données qui justifie le traitement différencié qui leur est accordé⁴. De telles données présentent, en outre, un risque d'affecter la sphère la plus intime des sujets des données ainsi qu'un risque sérieux de dommage, en cas d'abus, pour la personne concernée⁵.

¹ Certaines parties de la présente contribution s'inspirent de la contribution co-écrite avec la Professeure Cécile de Terwangne : « Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution », *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, pag. mult. This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreements n° 688520 (TeSLA). La publication ne reflète que l'opinion de son auteur et la Commission européenne ne peut être tenue responsable de l'usage qui en serait fait.

² Directeur de recherches au CRIDS (www.crids.eu) et avocat au barreau de Bruxelles (www.rawlingsgiles.be).

³ L'auteur remercie Jean Herveg et Karen Rosier pour leur relecture attentive de la présente contribution et leurs conseils avisés ainsi que les membres du CRIDS pour les fructueuses discussions.

⁴ Voy. J. RINGELHEIM, « Recueil des données personnelles et lutte contre les discriminations. Une tension nécessaire entre non-discrimination et vie privée », in *Les nouvelles lois luttant contre la discrimination*, Bruges, la Chartre, 2008, pp. 91 et s.

⁵ Voy. les développements consacrés à la raison d'être de la catégorie spécifique des données sensibles dans C. DE TERWANGNE et J.-Ph. MOINY, « La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et les concepts fondamentaux de la protection des données », *Vie privée et données à caractère personnel*, *op. cit.*, pt 6.

LE RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Le RGPD consacre deux articles à ce type de données selon une division assez logique mettant en place un régime général d'interdiction :

- D'une part, les données à caractère personnel dont le traitement « révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique »⁶ ;

À noter que cet article prévoit une série de bases de licéité fixée par le législateur européen, à savoir :

« [Le principe d'interdiction de traitement] ne s'applique pas si l'une des conditions suivantes est remplie

- a) 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 ;
- b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ;
- c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données

⁶ Art. 9 du RGPD.

LES CATÉGORIES PARTICULIÈRES DE DONNÉES À CARACTÈRE PERSONNEL

- à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées ;
- e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;
 - f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;
 - g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;
 - h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3 ;
 - i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tel que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;
 - j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ».

LE RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

- D'autre part, les données « relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes »⁷.

2. Pour situer la place de ces deux articles dans l'analyse du RGPD, il est utile de signaler que leur analyse doit être effectuée dans le cadre du paragraphe 1^{er} de l'article 5. En effet, la lecture doit être la suivante afin qu'elle soit plus facile à aborder :

- vérifier que les données soient traitées loyalement et licitement tel que cela est prescrit par l'article 5, § 1, a), du RGPD ;
- vérifier que les finalités soient déterminées, explicites et légitimes ainsi que le paragraphe 1, b), de l'article 5 le prévoit ;
- appliquer les articles 6, 9 et 10 selon le type de données à caractère personnel pour vérifier les bases de licéité présumées ;
- cette étape accomplie, revenir à l'article 6, 1, pour vérifier que les données soient bien pertinentes, adéquates, etc.

Il s'agit d'un "jeu de piste", mais qui doit être "joué" dans cet ordre pour pouvoir arriver à une solution qui soit compatible avec le RGPD.

3. Dans la présente contribution, nous allons aborder les éléments susceptibles de soulever des questions dans la mise en œuvre de ces articles 9 et 10 du RGPD après avoir présenté certaines définitions relatives aux données particulières dont il est question dans ces deux articles.

CHAPITRE 1. Définitions

4. Palliant une des carences de la directive 95/46/CE 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 (directive 95/46/CE ci-après), le RGPD définit certaines données particulières telles que les données génétiques, les données biométriques et les données concernant la santé.

⁷ Art. 10 du RGPD. L'article 6 du RGPD traite de la licéité du traitement de données non particulières ou sensibles.

SECTION 1. – Données génétiques

5. Le RGPD définit les données génétiques comme étant « les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question »⁸.

Il est heureux que le RGPD intègre ce type de données dans la catégorie particulière ce qui permet d'éviter de devoir trouver des solutions bricolées afin d'offrir à ces données une protection adéquate. En termes de solution, l'on assimilait souvent une donnée génétique à une donnée relative à la santé afin de la considérer comme sensible au sens de l'article 8 de la directive 95/46. En effet, ces données sont aussi fréquemment utilisées dans une optique de santé.

La question se posait également lorsque de telles données étaient traitées dans un cadre judiciaire. Le traitement n'avait pas de finalité médicale, mais bien d'identification de l'auteur d'un délit ou, dans le cadre d'action en recherche de paternité, du père d'un enfant. Si, dans la première hypothèse, l'on pouvait considérer qu'il s'agissait de données relatives à une infraction, tel n'était pas le cas dans la seconde.

Le RGPD enlève toute ambiguïté à ce niveau en considérant que ce type de données doit faire l'objet d'une protection accrue via l'article 9.

6. La Commission Nationale Informatique et libertés a précisé certains aspects de ces données qui les rendent particulières :

« Les données génétiques ne sont pas des données personnelles comme les autres. Particulièrement intimes et potentiellement discriminantes, ces données bénéficient d'un statut légal très protecteur.

Les données génétiques sont des informations relatives aux caractéristiques génétiques qui donnent des informations uniques sur la physiologie ou l'état de santé.

Or, l'exploitation de ces données, initialement circonscrite à la sphère médicale et à l'identification judiciaire tend à se développer dans des domaines de plus en plus diversifiés : assurances, généalogie, marketing, lutte contre l'immigration...

Les enjeux éthiques n'ont jamais été aussi importants : risques de manipulation génétique et de discrimination, maîtrise de son patrimoine génétique, marchandisation des données etc. »⁹.

⁸ Art. 4, 13, du RGPD.

⁹ CNIL, *Les Données génétiques*, Point CNIL, 2017.

LE RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Il est utile de relever que, si une définition de la notion de données génétiques avait déjà été donnée par la recommandation R(97) 5 du 13 février 1997 relative à la protection des données médicales¹⁰ qui était axée sur le caractère d'appartenance à un groupe d'individus, celle du RGPD tient compte des avancées scientifiques notables depuis 1997.

Afin de mieux cerner la définition, l'on doit se référer au considérant 34 qui précise que :

« Les données génétiques devraient être définies comme les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique, résultant de l'analyse d'un échantillon biologique de la personne physique en question, notamment une analyse des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou de l'analyse d'un autre élément permettant d'obtenir des informations équivalentes ».

À noter que le RGPD, à l'instar de la Directive 95/45 avant lui, se veut technologiquement neutre, ce qui se retrouve dans cette définition par l'utilisation des termes « analyse d'un autre élément permettant d'obtenir des informations équivalentes ».

7. L'on doit cependant se poser la question de savoir ce que l'on n'entend par « personne concernée ».

Selon le RGPD, la personne concernée est la personne physique identifiée ou identifiable par les données à caractère personnel¹¹, les informations génétiques en l'espèce. Or, les informations génétiques permettent d'identifier plusieurs personnes dès lors que, selon la Conseil de l'Europe, elles « concernent les caractères héréditaires d'un individu ou qui sont en rapport avec de tels caractères formant le patrimoine d'un groupe d'individus apparentés »¹². Ces informations concernent donc bien plus de personnes que celle sur laquelle a été prélevé l'ADN.

¹⁰ Recommandation du Conseil de l'Europe R(97), 5 du 13 février 1997 relative à la protection des données médicales : « l'expression « données génétiques » se réfère à toutes les données, quel qu'en soit le type, qui concernent les caractères héréditaires d'un individu ou qui sont en rapport avec de tels caractères formant le patrimoine d'un groupe d'individus apparentés.

Elle se réfère également à toute donnée portant sur l'échange de toute information génétique (gènes) concernant un individu ou une lignée génétique, en rapport avec les aspects, quels qu'ils soient, de la santé ou d'une maladie, qu'elle constitue ou non un caractère identifiable.

La lignée génétique est constituée par des similitudes génétiques résultant d'une procréation et partagées par deux ou plusieurs individus ».

¹¹ Voy. art. 2.a de la directive 95/46/CE.

¹² Recommandation n° R(97)5 du Conseil de l'Europe.

Le Groupe 29¹³ a fort bien résumé cela en déclarant que :

« une des caractéristiques fondamentales des données génétiques consiste à la fois dans le marquage distinctif d'un individu par rapport aux autres et dans le fait que ces données - et plus précisément : les caractéristiques auxquelles elles se réfèrent - sont partagées structurellement par tous les membres du même groupe biologique - tandis que d'autres mécanismes par lesquels les données personnelles sont partagées dépendent de la volonté de la personne concernée, de la coutume sociale, ou des règles juridiques »¹⁴.

Doit-on dès lors utiliser le singulier ou le pluriel pour parler de la personne concernée ?

Le Groupe 29 n'a pas tranché la question, mais a exposé deux scénarii possibles :

« Suivant le premier, les autres membres de la famille pourraient également être considérés comme « personnes concernées » disposant de tous les droits qui en découlent. Une autre option voudrait que les autres membres de la famille disposent d'un droit à l'information d'une nature différente, sur la base du fait que leurs intérêts personnels peuvent être directement affectés. Toutefois, dans les deux scénarios, de nouvelles options et conditions devraient être envisagées pour tenir compte des divers conflits susceptibles de surgir entre les différentes revendications des membres de la famille, visant soit à accéder à l'information soit à maintenir celle-ci confidentielle »^{15,16}.

Si la seconde piste est séduisante, elle ne correspond cependant pas à l'économie du RGPD et à la définition de « personne concernée » qu'elle donne. Pour rappel, le considérant 26 précise que « Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour

¹³ Devenu le Comité européen de la protection des données avec le RGPD.

¹⁴ Groupe 29, Document de travail sur les données génétiques, 17 mars 2004, WP 91, p. 8.

¹⁵ *Ibid.*

¹⁶ Il est intéressant de relever que la Commission de la protection des données italienne (Garante per la protezione dei dati personali) « qui a accordé à une dame la possibilité d'accéder aux données génétiques de son père bien que ce dernier n'ait pas accordé son consentement » en se basant, en substance sur une prévalence du droit de la dame sur celui de son père. Cette demande a été accordée au motif que le droit du père à la confidentialité ne pouvait prévaloir sur le droit de la dame à la santé – ce dernier signifiant son « bien-être psychologique et physique ».

identifier la personne physique directement ou indirectement, tels que le ciblage ».

Or, une analyse ADN produit nécessairement des informations afférentes à d'autres personnes que celle ayant donné l'échantillon ADN. Cette caractéristique est lourde de conséquences si cela implique que le responsable du traitement doit accorder à ces tiers le statut de personne concernée – au même titre qu'à la personne ayant fait l'objet du prélèvement – avec, en corollaire, la même protection avec d'éventuels conflits d'intérêts que nous verrons ci-dessous¹⁷.

SECTION 2. – Données biométriques

8. Le RGPD définit les données biométriques comme étant « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques »¹⁸.

Pour circonscrire cette définition, il convient de se référer au considérant n° 51 qui précise que :

« Le traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique ».

En d'autres termes, pour être considérées comme données biométriques, il faut que le traitement qui est fait des données permette ou confirme l'identification unique de la personne concernée, ce qui n'est pas le cas d'une simple photo.

¹⁷ Voy. Chapitre 2, Section 3, § 1.

¹⁸ Art. 4, 14, du RGPD.

SECTION 3. – Données concernant la santé

9. Le RGPD définit les données concernant la santé comme étant « 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 »¹⁹.

Cette définition est plus large que ce qui figurait dans la directive 95/46/CE car elle ne couvre plus les données **relatives** à la santé, mais qui **révèlent** des informations sur l'état de santé²⁰. Cela revient à dire que, dès qu'une donnée révèle un état de santé de la manière la plus infime possible, elle est une donnée particulière au sens du RGPD.

À noter que la recommandation R (97)5 du Comité des Ministres du Conseil de l'Europe a utilisé la notion de « données médicales » qui « se réfère à toutes les données à caractère personnel relatives à la santé »²¹ ce que certains auteurs considèrent comme moins large que la notion de *révéler* choisie par le RGPD²². Cependant le Conseil de l'Europe pourrait adopter la même définition que celle du RGPD tel que cela ressort de son projet de recommandation en matière de protection des données relatives à la santé du 8 juin 2018²³.

¹⁹ Art. 4, 15, du RGPD.

²⁰ Voy. les développements consacrés par Yves Poulet et Thierry Léonard à la portée de cette définition, ainsi que la critique que ces auteurs émettent en déplorant qu'on ne tienne pas plutôt compte de l'objectif des traitements effectués sur ces données pour déterminer leur caractère sensible ou non : Y. POULLET et Th. LÉONARD, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, p. 386.

²¹ Recommandation R(97) 5 du 13 février 1997 relative à la protection des données médicales.

²² Voy. à ce sujet, M. BOULANGER, S. CALLENS et S. BRILLON, « La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001 », *T. Gez.-Rev. dr. santé*, 2000-2001, p. 331 ; *ibid.*, pp. 326 et s. ; M. PARISSÉ et V. VERBRUGGEN, « Secret professionnel et vie privée : les traitements de données à caractère personnel (relatives à la santé) couvertes par le secret professionnel », *R.D.T.I.*, 2006, pp. 15 et s. ; J. DHONT, « Le traitement des données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, 2000/1, p. 302 et note 33 ; J. DHONT et Y. POULLET, « De verwerking van medische persoonsgegevens voor wetenschappelijke en statistische doeleinden », *D.W.T.C.*, 1998, pp. 28 et s.

²³ Non publié.

Pour sa part, le Groupe 29 a précisé dans un avis du 15 février 2007²⁴ que :

« L'indication du fait qu'une personne s'est blessée au pied et est à temps partiel pour raisons médicales constitue une donnée à caractère personnel relative à la santé au sens de l'article 8, paragraphe 1, de la directive [95/46]. Cette définition s'applique également aux données à caractère personnel lorsqu'elles présentent un lien clair et étroit avec la description de l'état de santé d'une personne : les données sur la consommation de médicaments, d'alcool ou de drogue et les données génétiques sont incontestablement des "données à caractère personnel relatives à la santé", en particulier si elles sont consignées dans un dossier médical. En outre, toutes autres données – par exemple des données administratives (numéro de sécurité sociale, date d'admission à l'hôpital, etc.) – contenues dans les documents médicaux relatifs au traitement d'un patient doivent être considérées comme sensibles : si elles n'étaient pas pertinentes dans le cadre du traitement du patient, elles n'auraient pas été, et n'auraient pas dû être, incluses dans un dossier médical ».

Il est à noter que la personne concernée par des données relatives à la santé est le patient lui-même, et non ses héritiers²⁵.

10. Dans l'affaire *Lindqvist* confiée à la Cour de justice de l'Union européenne²⁶, le ministère public, suivi par le juge suédois qui prononça la condamnation initiale à l'origine de l'affaire, a reproché à M^{me} Lindqvist d'avoir traité sans autorisation des données à caractère personnel sensibles, « à savoir celles relatives à une blessure au pied et à un congé de maladie [d'une de ses collègues] »²⁷. La juridiction d'appel voulut obtenir la confirmation que l'indication du fait qu'une personne s'est blessée au pied et est en congé de maladie partiel constitue bien une donnée à caractère personnel relative à la santé au sens de l'article 8 de la directive. La Cour de Luxembourg ne tergiversa pas sur cette question de détermination de

²⁴ Groupe 29, Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), WP 131, 15 février 2007, p. 8.

²⁵ Cela a été affirmé par le Tribunal de première instance de Bruxelles qui, dans le cadre de l'article 7 de la loi vie privée, remplacée aujourd'hui par le RGPD, a estimé que les ayants droit d'un patient décédé doivent être considérés comme des tiers par rapport à la personne concernée qu'était le défunt (Civ. Bruxelles, 25 mars 2005, *J.L.M.B.*, 2005, p. 1197).

²⁶ C. DE TERWANGNE, « Arrêt *Lindqvist* ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., 6 novembre 2003, *R.D.T.I.*, 2004, n° 19, pp. 67 à 99.

²⁷ Pt 15 de l'arrêt.

cette catégorie particulière de données. Elle répondit qu'il convient de réserver une interprétation large à l'expression « données relatives à la santé ». Cela conduit à faire entrer dans cette catégorie les informations portant sur « tous les aspects, tant physiques que psychiques, de la santé d'une personne »²⁸. Et la Cour de conclure que la mention du pied blessé et du congé de maladie subséquent relève effectivement de cette catégorie.

Selon le Conseil d'État belge, « un test d'haleine implique le traitement de données de santé »²⁹.

11. Pour le surplus, nous renvoyons à la partie du présent ouvrage consacré à « l'impact du Règlement général sur la protection des données dans le secteur de la santé » dans laquelle il est procédé à une analyse plus approfondie de la notion de données relatives à la santé.

CHAPITRE 2. L'article 9 du RGPD

Préambule³⁰

12. Ainsi que nous l'avons précisé précédemment pour ce qui concerne les données relatives à la santé³¹, la question des données sensibles suscite l'éternel débat entre tenants de l'hypothèse où c'est le contexte d'utilisation, la finalité du traitement envisagé qui rend les données sensibles et ceux qui estiment indispensable d'établir une liste de données sensibles par nature. Le recours à une telle liste déclenche automatiquement l'application d'un régime de protection renforcé lié au risque d'affecter la sphère la plus intime des individus ou d'engendrer des discriminations illégitimes ou arbitraires sur la base des données visées. Une telle liste permet donc d'évacuer toute interrogation contextuelle.

La définition des données sensibles présentée sous forme de liste à l'article 9 du RGPD n'est pas sans susciter un certain malaise. La formulation est effectivement extrêmement large du fait que sont couvertes

²⁸ Pt 50 de l'arrêt.

²⁹ C.E., 27 octobre 2005, n° 150.861, cité par J.-Ph. MOINY et J.-M. VAN GYSEGHEM, « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, 2009, p. 90.

³⁰ Le présent préambule a déjà été, en partie, exposé dans C. DE TERWANGNE et J.-M. VAN GYSEGHEM, « Analyse détaillée de la loi de protection des données et de son arrêté royal d'exécution », *Vie privée et données à caractère personnel*, Bruxelles, Politeia, 2013, pag. mult

³¹ Voy. Chapitre 1, Section 3.

LE RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

par le régime particulier les « données à caractère personnel relatives à l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, [...] »³². Cela signifie en effet, que tombent dans cette catégorie, par exemple, les noms patronymiques qui révèlent indubitablement l'origine raciale, de même que toute photo d'une personne ; l'achat d'un ouvrage de la bible sur un site web peut quant à lui révéler les convictions religieuses, etc. Or, il est inconcevable de traiter systématiquement les noms, les photographies et certains achats comme des données sensibles bénéficiant d'un régime de protection particulièrement sévère. Ce ne sera que quand c'est justement l'élément sensible de la donnée qui est retenu par le responsable du traitement (sélection des personnes d'origine russe ou japonaise, sur la base de leurs noms ; ou sélection des personnes de type maghrébin, tutsi, rom ou aborigène sur la base de leurs photos) que le régime protecteur, principalement lié au risque élevé de discrimination à partir des données traitées, se justifie³³. C'est pour contrer un risque de discrimination de ce type lors des embauches que se développe la pratique de sélectionner les candidats à un poste professionnel sur la base de curriculum vitae sans nom apparent.

D'une part, il est louable de retenir les données relatives à des caractéristiques sensibles des personnes. Cela permet en effet de considérer comme sensibles des cas dans lesquels n'apparaît aucune donnée *a priori* sensible. Ainsi, les recherches sur Google de sites sur le pèlerinage de Saint-Jacques-de-Compostelle pratiquées par un internaute, son achat de livres religieux, sa lecture d'une encyclique pontificale, etc. pourraient être traitées comme révélant une opinion religieuse.

D'autre part, retenir justement tout ce qui est relatif à une caractéristique sensible en arrive, ainsi qu'on l'a dit, à faire entrer dans cette catégorie de données énormément de données qui dans bien des cas ne sont pas traitées pour l'aspect sensible qu'elles véhiculent. Cela est excessif et risque d'ôter son sens à la notion de données sensibles au niveau de l'application concrète.

La Commission de la Protection de la Vie Privée belge devenue, depuis le 25 mai 2018, l'Autorité de protection des données a adopté plusieurs avis qui reflètent cette difficulté. Lors des auditions au Sénat précédant l'adoption de la législation en matière de vidéosurveillance, le président de la Commission l'a affirmé : « toute information n'est pas forcément

³² C'est nous qui soulignons.

³³ Voy. dans le même sens Th. 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/CE du 24 octobre 1995 », *J.T.*, 1999, p. 386, spéc. la note 106.

sensible en elle-même, ces caractéristiques pouvant résulter du contexte et des finalités pour lesquelles les données sont traitées. Ainsi, la couleur de la peau des personnes filmées, qu'elle soit blanche ou noire, ne peut être considérée comme sensible en elle-même, mais elle le serait si par exemple l'objectif de l'enregistrement d'images était d'identifier et de classer les personnes filmées selon leur couleur de peau »³⁴. À plusieurs reprises, la Commission avait déjà considéré que, si l'on pouvait déduire une information relative à l'état de santé d'une personne sur la base du port de lunettes ou d'un bandage autour du bras de la personne, ces images ne devaient pas être assimilées à des données médicales à caractère personnel dans les cas où ces caractéristiques ne sont pas utilisées pour en déduire systématiquement une information sur l'état de santé des personnes identifiées³⁵.

Le Comité sectoriel de la Commission de la Protection de la vie privée belge a réitéré cette position en faveur d'une prise en compte du contexte, de la finalité d'utilisation des données en cause avant de leur appliquer le régime des données sensibles. Le Comité sectoriel était saisi d'une demande portant sur la communication au Service des Pensions du Secteur Public de l'information relative au statut de grand invalide de guerre accordé à certaines personnes concernées. Le Comité a estimé que :

« Si l'on interprète l'article 7, § 1 de la LVP de façon stricte [ndr : article 7 de la loi belge du 8 décembre 1992 transposant l'article 8 de la Directive 95/46], cette information pourrait le cas échéant être qualifiée de donnée à caractère personnel relative à la santé. Le comité estime toutefois qu'une telle donnée n'est pas en soi nécessairement sensible, mais que son caractère sensible résulte éventuellement du contexte et des finalités pour lesquelles les données sont traitées. Étant donné que le présent traitement du demandeur s'inscrit dans un contexte purement administratif et n'a en outre pour but que d'octroyer un avantage fiscal aux personnes concernées, le comité estime [...] qu'il ne s'agit en

³⁴ Audition de MM. Michel Parisse et Willem De Beuckelaer, président et vice-président de la commission de la protection de la vie privée, Surveillance par caméra, Rapport, Sén., 2005-2006, *Document législatif* n° 3-1413/1.

³⁵ CPVP, Avis n° 14/95 du 7 juin 1995 sur l'applicabilité de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel à l'enregistrement d'images et ses conséquences ; CPVP, Recommandation n° 01/98 du 14 décembre 1998 en matière de Système Informatisé de Réservation ; CPVP, Avis n° 17/99 du 10 mai 1999 relatif au projet d'arrêté royal concernant l'installation et le fonctionnement de caméras de surveillance dans les stades de football.

LE RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

l'occurrence pas d'une donnée à caractère personnel relative à la santé et donc qu'aucun régime de protection plus strict ne s'applique »³⁶.

En 2012, la Commission de la protection de la vie privée belge a maintenu son approche contextualisée dans un avis portant sur les tests d'alcoolémie ou de détection de drogues³⁷. Elle a ainsi affirmé :

« La question de savoir si et dans quelles circonstances concrètes le résultat d'un test individuel d'alcoolémie ou de détection de drogues (qui ne constitue pas un traitement médical) doit être considéré comme une donnée relative à la santé ne doit *a priori* pas être examinée ici. Certaines données sont par nature des données relatives à la santé, d'autres permettent seulement potentiellement de déduire des informations relatives à l'état de santé physique ou psychique antérieur, actuel ou futur de la personne concernée. Dans les cas où le traitement des résultats des tests constitue un traitement de données relatives à la santé, la Commission estime que cela peut et doit se faire dans le cadre de l'article 7 de la LVP [ndr : article 7 de la loi belge du 8 décembre 1992 transposant l'article 8 de la Directive 95/46]. Il est clair que l'employeur qui fait subir à un membre du personnel, pendant une certaine période, plusieurs tests d'alcoolémie et/ou de détection de drogues dans le but, après un certain temps, de confirmer (ou de voir réfutés) ses soupçons que la personne concernée a un problème d'alcool ou de drogue, procède à un traitement de données relatives à la santé au sens de l'article 7 de la LVP. L'élément déterminant n'est pas le nombre de tests subis, mais la manière dont les résultats sont utilisés »³⁸.

³⁶ Comité sectoriel pour l'Autorité Fédérale, Délibération AF n° 10/2008 du 20 novembre 2008 concernant une demande d'autorisation formulée par l'Agence « Vlaamse Belastingdienst » (VLABEL) (Service flamand des Impôts) en vue du traitement de données à caractère personnel enregistrées dans des banques de données de l'Administration générale de la Documentation patrimoniale et du Service des pensions du secteur public.

³⁷ CPVP, Avis n° 36/2012 du 12 décembre 2012 concernant un avant-projet de loi portant certaines dispositions du statut administratif du personnel opérationnel des zones de secours et le livre 15 d'un avant-projet d'arrêté royal relatif au statut administratif du personnel opérationnel des zones de secours, portant sur l'exécution d'un test d'alcoolémie ou de détection de drogues (CO-A-2012-043).

³⁸ *Ibid.*

SECTION 1. – Le principe : l’interdiction de traitement

13. Le paragraphe 1^{er} de l’article 9 prescrit que « le traitement des données à caractère personnel qui révèle l’origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l’appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d’identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l’orientation sexuelle d’une personne physique sont interdits ».

Il s’agit d’un régime d’interdiction générale dicté par le fait que les données visées sont susceptibles *in se* de porter atteinte aux libertés fondamentales ou à la vie privée.

Cette interdiction générale s’avère très large et, ainsi qu’on l’a dit dans le préambule, cela engendre une difficulté majeure pour en déterminer la portée exacte. En effet, l’article 9 du RGPD est applicable dès l’instant où l’on traite les données y reprises, même si le traitement ne vise pas les données à caractère personnel pour l’élément sensible qu’elles comportent.

14. L’analyse du considérant n° 35 du RGPD pourrait cependant nous permettre de considérer que l’interdiction de traitement soit le principe pour les données à caractère personnel particulières, dont celles relatives à la santé, si elles sont traitées *pour ce qu’elles révèlent ou contiennent* :

« 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. Cela comprend des informations sur la personne physique collectées lors de l’inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil (1) au bénéfice de cette personne physique ; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l’identifier de manière unique à des fins de santé ; des informations obtenues lors du test ou de l’examen d’une partie du corps ou d’une substance corporelle, y compris à partir de données génétiques et d’échantillons biologiques ; et 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

LE RÉGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro ».

L'on constate que les traitements invoqués sont toujours en relation avec des soins de santé ou, à tout le moins, avec la santé.

Par ailleurs, le Groupe 29, s'est penché sur la question des informations sensibles pouvant découler d'une photographie d'une personne identifiable et a conclu que :

« Dans certains États membres de l'Union européenne, les images de personnes concernées sont considérées comme une catégorie spéciale de données personnelles puisqu'elles peuvent être utilisées pour distinguer l'origine raciale/ethnique ou pour en déduire des croyances religieuses ou des données relatives à la santé. Le groupe de travail ne considère pas, en général, les images sur Internet comme des données sensibles, sauf si elles sont clairement utilisées pour révéler des données sensibles sur des personnes »³⁹.

Une analyse similaire pourrait être opérée pour les autres données visées par l'article 9 dès lors que l'on se retrouve, à chaque fois, dans une situation identique. En effet, il en va de même pour les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique.

Il est intéressant de noter que le Conseil de l'Europe a, dans le cadre de modernisation de la Convention 108⁴⁰, considéré que les catégories particulières de données devaient être analysées au regard de leur traitement pour les informations qu'elles révèlent. En d'autres termes, cela revient à distinguer le contexte du traitement sous la réserve des données génétiques qui « peuvent comporter un risque particulier pour les personnes concernées, indépendamment du contexte du traitement »⁴¹.

En conclusion, il faut analyser cette définition au regard de la finalité poursuivie par le responsable du traitement. En effet, c'est cette finalité qui permettra de faire entrer le traitement dans l'article 9 ou dans l'article 6.

³⁹ Groupe 29, Avis 5/2009 du 12 juin 2009 sur les réseaux sociaux en ligne, WP 163.

⁴⁰ Convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0.

⁴¹ Voy. rapport explicatif de la Convention 108 modernisée, pt 57, p. 11.

Il convient à ce stade de préciser que par « origine raciale », le RGPD « n'implique pas que l'Union adhère à des théories tendant à établir l'existence de races humaines distinctes »⁴².

On attire l'attention sur le fait que, si l'on peut traiter les données de la première catégorie de données sensibles avec le consentement des personnes concernées, cela n'est pas admis pour le traitement de données « judiciaires » visées à l'article 10 du RGPD. Les possibilités de traitement de ces dernières données sont d'ailleurs beaucoup plus restreintes.

On relève également que la notion de nécessité est omniprésente dans les hypothèses d'exceptions admises.

Dans le cadre de la présente contribution, nous n'allons pas aborder toutes les exceptions visées à l'article 9, § 2, du RGPD dès lors que certaines soit ne soulèvent pas de difficultés majeures soit doivent faire l'objet de législations nationales précisant, entre autres, la notion d'« intérêt public » ou requérant des garanties sur la base de l'article 89 du RGPD⁴³.

SECTION 2. – Les exceptions au principe général d'interdiction

15. Si cet article 9 prescrit un principe général d'interdiction, il prévoit cependant des exceptions pour lesquelles le législateur européen a effectué une balance d'intérêts.

L'on doit rappeler le principe général selon lequel toute exception doit être interprétée de manière restrictive et, à tout le moins, dans les intérêts de la personne protégée qui est, dans le cadre du RGPD, la personne concernée.

Par ailleurs, il est utile de rappeler que le fait de se trouver dans le champ d'application d'une des exceptions de l'article 9 ne dispense pas le responsable du traitement de procéder à une information conformément au RGPD à moins qu'il n'en soit dispensé par le même RGPD ou une loi nationale. L'information à l'égard de la personne concernée est primordiale et doit porter sur toutes les finalités des traitements de données à caractère personnel, en ce compris les traitements ultérieurs. En outre, cette information doit être fournie dans un langage compris par l'utilisateur. Or, la lecture de nombreuses « *privacy policies* » montrent que la

⁴² Voy. considérant n° 51 du RGPD.

⁴³ Pour la Belgique, il faudra se référer à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

langue utilisée est l'anglais alors que le traitement porte sur des données de personnes n'ayant pas une bonne connaissance de cette langue. Aux clients ne lisant pas l'anglais échapperont donc certaines informations qui sont pourtant essentielles pour donner un consentement éclairé⁴⁴. Il est donc primordial que le responsable du traitement soit attentif au public qu'il vise afin d'adapter la langue utilisée en termes d'information en conséquence. Par ailleurs, l'on doit également être attentif aux réglementations nationales ou même régionales sur l'emploi des langues.

En clair, le responsable du traitement n'est, en rien, dispensé de respecter ces obligations.

§ 1. Le consentement de la personne concernée

16. Le paragraphe 2, a), de l'article 9 du RGPD prévoit que les données particulières pourront 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 ».

Rappelons que, pour être valable, le consentement doit avoir été donné sans pression aucune (consentement libre), en toute connaissance de cause (consentement éclairé) et de manière spécifique et non générale (consentement spécifique). Le RGPD précise à son article 7 que le consentement donné par une personne concernée doit pouvoir à tout moment être retiré par celle-ci.

Cette exception n'est toutefois plus valable lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement l'empêchant de refuser librement son consentement.

17. Par ailleurs, le consentement peut révéler des situations inconfortables. Ainsi, il en va des données génétiques avec la multiplicité des personnes susceptibles d'être considérées comme concernées au sens du RGPD. La question posée est évidemment de savoir si la personne est identifiée ou identifiable ainsi que nous l'avons déjà exposé ci-dessus⁴⁵. En règle générale, les personnes concernées par le traitement des

⁴⁴ Cette notion a déjà été développée dans J.-M. VAN GYSEGHEM, « L'économie collaborative et la protection des données : quel partage de données ? », *Aspects juridiques de l'économie collaborative*, Limal, Anthemis, 2017, pp. 251-275 (Les dossiers du BJS).

⁴⁵ Voy. Chapitre 1, Section 1.

informations génétiques sont connues ou peuvent l'être assez aisément. En effet, dans la plupart des cas, les ascendants, descendants ou collatéraux de la personne concernée dont est issu l'ADN sont connus. Ces ascendants, descendants et collatéraux identifiables et identifiés doivent être considérés comme personnes concernées⁴⁶. Seules certaines hypothèses rendent cette connaissance difficile telle la naissance sous X, l'adoption suite à un abandon, etc.

L'analyse des conséquences pratiques de cette multiplicité de personnes concernées part de l'hypothèse que nous avons deux personnes concernées dont une pour laquelle un traitement de données est nécessaire donne son consentement tandis que l'autre le refuse. Nous sommes donc face à deux personnes qui ont les mêmes droits, mais dont l'exercice est antagoniste avec pour conséquence que le traitement ne sera pas possible compte tenu de la multiplicité des personnes concernées qui ont des droits équivalents avec cependant une prévalence du refus dès lors que nous sommes en présence de catégories particulières de données. Le RGPD n'offre pas de solution à ce type de situation, à moins que l'on soit dans une situation ne requérant pas le consentement, et il faudra donc se retourner vers la législation nationale en matière, par exemple, d'état de nécessité (pénal) ou d'abus de droit (civil) pour permettre le traitement.

En outre, le RGPD ne permet pas de balance d'intérêts entre deux personnes concernées, mais uniquement entre personnes concernées et responsable du traitement⁴⁷.

18. Pour le surplus, nous renvoyons au chapitre consacré au consentement pour de plus amples développements.

§ 2. Exécution des obligations du responsable du traitement ou de la personne concernée

19. La deuxième exception s'applique dès lors que « le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par

⁴⁶ Dans l'hypothèse où il est extrêmement difficile d'identifier ces personnes, il convient de considérer que les droits et obligations contenus dans le Règlement sont suspendus aussi longtemps que ces personnes restent non identifiées dès lors que l'on sait que d'autres personnes sont concernées par le traitement, mais qu'elles ne sont pas encore identifiées.

⁴⁷ Art. 6, § 1, f), du RGPD.

le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée »⁴⁸.

Si la formulation de cet article fait penser au principe mis en place par l'article 6, 1, b), du RGPD⁴⁹, il se différencie par le fait que cette exception se limite aux seules matières de droit du travail, de la sécurité sociale et de la protection sociale. À noter cependant que le RGPD élargit le champ d'application de cette exception par rapport à que prévoyait la Directive qui le limitait au seul droit du travail.

20. La formulation et donc la limitation de cette exception de l'article 9, 2, b), du RGPD peuvent poser certains problèmes de mise en œuvre ou, à tout le moins, générer des comportements inattendus dans le chef de compagnies d'assurances. Ainsi, certaines ont envoyé des formulaires de consentement à leur client portant sur le traitement de données santé dans le cadre de produits d'assurance auxquels ces mêmes clients avaient souscrit. En effet, certains acteurs économiques proposent des services d'assurances impliquant le remboursement de frais de santé avec, comme conséquence, un traitement de données relatives à la santé. Dans cette situation particulière, l'on doit analyser ce traitement au regard des obligations de la compagnie d'assurances afin de vérifier si le traitement des données est conforme au RGPD.

L'on vient de préciser que le traitement ne peut s'effectuer dans le cadre d'un contrat qu'à condition qu'il soit en lien avec le droit du travail, de la sécurité sociale ou de la sécurité sociale. Or, en l'espèce, la fourniture de services ne s'inscrit pas dans ces matières. Doit-on dès lors considérer que cet acteur doit demander un consentement spécifique pour le traitement qu'il va effectuer pour rembourser les frais de soins de santé alors que c'est l'objet même du contrat ?

Si l'on se reporte au considérant n° 52 du RGPD qui précise que les « dérogations sont possibles à des fins de santé, en ce compris la santé publique et la gestion des services de soins de santé, en particulier pour assurer la qualité et l'efficacité des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie », nous pourrions répondre à la question posée. Si l'assurance-maladie n'est pas définie par le RGPD, l'on peut considérer que les assurances de types assurance hospitalisation ou ambulatoire entrent dans la notion d'« assurance-maladie ». Cette intégration est, à tout le moins, effectuée par

⁴⁸ Art. 9, § 2, b), du RGPD.

⁴⁹ « le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ».

l’Autorité des Services et Marchés Financiers belge (FSMA) qui précise, sur son site Internet WIKIFIN, que les composantes de l’assurance-maladie sont « L’assurance soins de santé », « L’assurance indemnités pour incapacité de travail ou invalidité », « L’assurance hospitalisation », « L’assurance ambulatoire », « L’assurance dépendance » et « l’assurance individuelle accident⁵⁰ ». En clair, les compagnies d’assurance offrant des produits tendant au remboursement de soins de santé à leurs assurés pourraient bénéficier de l’exception prévue à l’article 9, 2, b, du RGPD.

21. Si cette thèse ne peut être suivie, l’on pourrait alors considérer que la souscription du contrat d’assurance emporte consentement au traitement de données sans que la personne concernée doive donner un consentement distinct en se basant sur la notion d’« activité de base » par une analogie avec l’article 37 du RGPD dans lequel le législateur européen utilise le concept d’« activité de base » du responsable du traitement précisé au considérant 97 comme ayant « trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu’activité auxiliaire ».

Selon Groupe 29 :

« les « activités de base » peuvent être considérées comme les opérations essentielles nécessaires pour atteindre les objectifs du responsable du traitement ou du sous-traitant.

Toutefois, les « activités de base » ne doivent pas être interprétées comme excluant les activités pour lesquelles le traitement de données fait partie intégrante de l’activité du responsable du traitement ou du sous-traitant. Par exemple, l’activité de base d’un hôpital est de fournir des soins de santé. Toutefois, un hôpital ne peut fournir de soins de santé de manière sûre et efficace sans traiter des données concernant la santé, telles que les dossiers médicaux des patients. Par conséquent, le traitement de ces données doit être considéré comme l’une des activités de base de tout hôpital, et les hôpitaux doivent donc désigner un DPD ; »⁵¹.

S’il est vrai que cette analyse du Groupe 29 porte sur la notion d’« activité de base » liée à l’obligation de désignation d’un DPO, ne pourrions-nous effectuer une appropriation de cette notion dans l’analyse de l’article 9, 2, b), du RGPD pour éviter de procéder à une déconnexion d’un

⁵⁰ www.wikifin.be/fr/thematiques/assurer/assurance-maladie-et-accident/en-cas-de-maladie-ou-daccidents?gclid=EAlaIqObChMI34SP84jb2wIVVM0bCh09_QGoEAYASAAEgl-3_D_BwE.

⁵¹ Groupe 29, Lignes directrices concernant les délégués à la protection des données (DPD), WP 243 rev.01, adoptées le 13 décembre 2016 et révisées et adoptées le 5 avril 2017, p. 8.

contrat de base avec son objet essentiel ? Il serait, en effet, peu compréhensible, dans le chef de la personne concernée, assurée en l'espèce, de souscrire une assurance hospitalisation par exemple et de devoir, par ailleurs, donner un consentement pour que la compagnie d'assurance puisse traiter les données en vue du remboursement des frais de soins de santé qui est l'objet-même du contrat.

Il nous apprend donc conciliable avec l'esprit du RGPD que la souscription du contrat d'assurance permette à l'assurance de traiter de telles données.

Pour le surplus, nous renvoyons aux développements sur la notion de consentement exposés par Cécile de Terwangne dans la contribution intitulée « Les principes relatifs au traitement des données à caractère personnel et sa licéité ».

22. Une telle question ne se posera pas pour les mutuelles qui agissent, elle, dans le domaine de la sécurité sociale et donc peuvent bénéficier de l'exception de l'article 9, § 2, b), du RGPD. Cette analyse peut être déduite du considérant n° 52 qui précise que « ces dérogations sont possibles à des fins de santé, en ce compris la santé publique et la gestion des services de soins de santé, en particulier pour assurer la qualité et l'efficacité des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie ».

23. L'article 9, § 2, b), du RGPD prévoit également les traitements nécessaires « aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail ». Le RGPD n'est cependant pas très prolix quant à l'étendue que le législateur européen a voulu donner à cette notion de droit du travail. Peut-on, par exemple, considérer que le pointage des employés par l'utilisation de la biométrie demande un consentement préalable de l'employé ou peut-on considérer que cela entre dans l'obligation, pour l'employeur, de payer ses employés en fonction de leurs heures de travail ?

La question doit être analysée en deux étapes, à savoir la nécessité du traitement et l'étendue de la notion d'obligation du responsable du traitement en matière de droit du travail.

L'analyse de la nécessité renvoie nécessairement vers une notion qui trouve son origine dans l'article 8 de la Convention européenne des droits de l'homme. Ainsi que cela a déjà été mentionné par ailleurs dans le présent ouvrage, la finalité du traitement de données doit être « légitime », concept qui renvoie à la nécessité de respecter le principe de proportionnalité.

Cette exigence de finalité légitime doit se combiner avec l'exigence pour l'ensemble du traitement de respecter la règle de proportionnalité. Ainsi, la Commission européenne intervenant dans l'affaire *Österreichischer Rundfunk* confiée à la Cour européenne de justice, évoque « l'examen de proportionnalité effectué en vertu de l'article 6, paragraphe 1, sous b) [de la directive 95/46] »⁵².

Dans un arrêt du 10 novembre 2011⁵³, la Cour constitutionnelle belge a eu l'occasion de rappeler que « toute ingérence des autorités dans le droit au respect de la vie privée [doit être] prévue par une disposition législative suffisamment précise » outre qu'elle doit répondre « à un besoin social impérieux » et qu'elle doit être « proportionnée au but légitime qui est poursuivi ».

La Cour européenne des droits de l'homme a également estimé que « le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions, mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique »⁵⁴.

Dans son arrêt *Volker und Markus Scheke & Eifert*⁵⁵, la Cour de justice de l'Union européenne a considéré « que la publication sur Internet de données nominatives concernant les personnes physiques bénéficiaires d'aides agricoles constitue une ingérence dans leur droit au respect de la vie privée reconnu à l'article 7, et un traitement de données relevant de la protection garantie par l'article 8 de la Charte⁵⁶. Si cette ingérence peut être considérée comme poursuivant un but légitime, à savoir l'accroissement

⁵² C.J.C.E., 20 mai 2003, arrêt *Österreichischer Rundfunk e.a.*, C-465/00, C-138/01 et C-139/01, pt 57.

⁵³ C.C., 10 novembre 2011, 166/2011, www.const-court.be, B35.3. Il faut relever que cette exigence permet au justiciable de contrôler l'ingérence et sa légalité. Voy. égal. Cour eur. D.H., 4 mai 2000, arrêt *Rotaru c. Roumanie*, Rev. trim. dr. h., 2001, pp. 137-183, obs. O. DE SCHUTTER.

⁵⁴ Cour eur. D.H., 4 décembre 2008, arrêt *S. et Marper c. Royaume-Uni*, req. nos 30562/04 et 30566/04, <http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90052>, al. 125.

⁵⁵ C.J.U.E. (GC), 9 novembre 2011, arrêt *Volker und Markus Schecke GbR et Harmut Eifert c. Land Hessen*, aff. jointes C-92/09 et C-93/09. Voy. E. DEGRAVE, « Arrêt 'Volker und Markus Schecke et Eifert' : le droit fondamental à la protection des données à caractère personnel et la transparence administrative », *J.D.E.*, 2011, pp. 97-99.

⁵⁶ Pts 58 et 60.

de la transparence de l'utilisation des fonds communautaires de la PAC⁵⁷, elle sera finalement jugée disproportionnée par la Cour⁵⁸ »⁵⁹.

Lorsqu'il met en place un traitement de données biométriques à des fins de calcul des heures de travail des employés, l'employeur devra nécessairement se poser, outre la question de la licéité du traitement, celle de la proportionnalité. Il devra vérifier s'il n'existe pas des moyens de traitement engendrant une ingérence moins grande dans la vie privée de l'employé, par l'utilisation de badge nominatif par exemple. Si la réponse est positive, il ne pourra se prévaloir de l'exception de traitement prévue à l'article 9, 2, b), du RGPD dès lors que le traitement n'est pas nécessaire.

Si, par contre, la réponse à cette question est négative, il devra alors également justifier du fait que le traitement est mis en œuvre pour remplir des obligations qui lui sont propres. Pour reprendre l'exemple du pointage, celui-ci permet à l'employeur de payer la juste rémunération méritée et ainsi remplir une obligation lui incombant au regard du droit du travail.

Il en sera de même lorsqu'il traitera les données relatives à la santé de ses employés dans le cadre des congés de maladie, traitement qui entre dans la notion de droit du travail.

§ 3. Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique

24. L'article 9, § 2, c), du RGPD donne une importance particulière à la sauvegarde des intérêts vitaux de l'être humain que ce soit la personne concernée ou une autre.

Deux conditions sont requises pour que l'exception trouve à s'appliquer, à savoir, d'une part, un intérêt vital dans le chef de la personne concernée ou d'une autre personne physique et, d'autre part, un état d'incapacité à consentir dans son chef. Aucune des deux conditions n'est définie par le RGPD, mais il précise cependant que l'incapacité peut être tant juridique que physique avec un renvoi, nous semble-t-il vers l'arsenal juridique et jurisprudentiel de chaque État membre.

⁵⁷ Pt 71.

⁵⁸ Pt 86.

⁵⁹ C. GAYREL, « Chronique de jurisprudence en droit des technologies de l'information (2009-2011). Libertés et société de l'information. Cour de Justice de l'Union Européenne, Tribunal de Première Instance et Tribunal de la Fonction Publique européenne », *R.D.T.I.*, 2012, n° 48-49, p. 107.

Cet article met en place le principe du « bris de glace » qui pourrait cependant faire l'objet d'un contrôle de validité *a posteriori*. Si la situation paraît assez évidente à mettre en œuvre, elle pourrait cependant donner lieu à des conflits d'intérêts.

§ 4. Activités légitimes de certaines fondations, associations et organismes à but non lucratif

25. Le RGPD consacre une place particulière aux fondation, association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, en leur permettant de traiter des données sensibles.

Il ne s'agit cependant pas d'un « blanc-seing » dès lors que le RGPD soumet cette exception à plusieurs conditions **cumulatives** :

- l'entité concernée doit être à but non lucratif. Il conviendra dès lors de vérifier, dans chaque État membre dans lequel la personne morale a son établissement principal la forme juridique qu'elle doit adopter ;
- la finalité poursuivie par cette entité doit être politique, philosophique, religieuse ou syndicale ;
- le traitement doit se rapporter « exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités [ndr : politique, philosophique, religieuse ou syndicale] »⁶⁰ ;
- les données ne peuvent pas être communiquées en dehors de cet organisme sans le consentement des personnes concernées.

En outre, ce traitement doit être accompagné de garanties appropriées qui devraient être, à notre sens et à défaut du RGPD, fixées par les États membres.

§ 5. Constatation, exercice ou défense d'un droit en justice

26. Dans le cadre du travail effectué par les cours et tribunaux comme acteurs de justice, il est inévitable que des données reprises dans le champ d'application de l'article 9, § 2, f), du RGPD soient traitées, ce qui rend une telle exception indispensable.

Le RGPD ne détermine pas les responsables de traitement pouvant bénéficier de cette exception, mais certains viennent cependant spontanément

⁶⁰ Art. 9, § 2, d), du RGPD.

à l'esprit tels les avocats dans l'exercice de leur mission d'acteur du monde judiciaire.

27. Les données particulières, à condition que leur traitement soit nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice, peuvent être traitées par des avocats, que ce soit des données relatives à leur client ou à un tiers, et ce, sans devoir requérir leur consentement.

Si certains considèrent que le consentement serait leur base de licéité du traitement, cette position est difficilement compatible lorsque l'avocat est amené à traiter les données de tiers autres que son client, telle la partie adverse. L'on imagine, en effet, assez mal que l'avocat aille solliciter le consentement de cette partie adverse avant de traiter les données la concernant avec le risque, d'une part, de violer son obligation au secret professionnel et, d'autre part, de porter préjudice aux intérêts de son propre client. L'avocat s'appuiera donc sur cette exception pour traiter les données nécessaires à la défense des intérêts de son client.

Ainsi que nous l'avons déjà mentionné ci-dessus, le fait que ces données puissent être traitées par l'avocat sans le consentement ne dispense pas de délivrer une information complète à son client. Bien évidemment et pour les mêmes raisons que celles invoquées dans le cadre de l'analyse du consentement ci-dessus, l'information ne doit pas être délivrée aux parties adverses – sous réserve d'une bonne administration de la justice et du principe du contradictoire –, et ce, en vertu d' « une impossibilité fonctionnelle (l'information contrarierait l'œuvre de l'avocat) et légale (l'information emporterait violation du secret professionnel) »⁶¹, mais également sur la base de l'article 14, § 5, d) du RGPD qui prévoit une exception à l'information si « les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membres, y compris une obligation légale de secret professionnel ».

28. Une telle exception vaut également pour les cours et tribunaux dans le cadre de leur fonction juridictionnelle ou administrative tel que cela est précisé par l'utilisation des mots « chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ».

Il nous semble que cela s'étende également à leurs auxiliaires. Nous pensons plus particulièrement aux experts désignés par le tribunal. À notre

⁶¹ C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *Cabinets d'avocats et technologies de l'information*, Cahiers du CRIDS, n° 26, 2005, p. 171.

sens, ils interviennent dans le cadre d'un mandat judiciaire et entrent donc dans le champ d'application de l'exception. Leur seule présence dans un procès est due à leur désignation comme expert, sous réserve de la distinction entre responsable du traitement et sous-traitant qui est analysée dans le chapitre consacré à « l'impact du Règlement général sur la protection des données dans le secteur de la santé ».

29. L'on peut également se poser la question quant aux médecins-conseils qui interviennent aux côtés d'un avocat dans un dossier. S'ils sont considérés comme responsables de traitements, il nous apparaît logique que le traitement qu'ils effectuent entre dans la notion de « traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ».

Par contre, s'ils sont considérés comme sous-traitants, il nous semble qu'ils tirent leur autorisation de traitement du fait qu'ils interviendront pour le compte et sous les instructions de l'avocat qui fait appel à leur service. En effet, le traitement qu'ils effectueraient n'est pas pour eux-mêmes, mais bien pour l'avocat qui leur donnera des instructions.

Cet aspect sera analysé de manière plus approfondie dans le chapitre consacré à « l'impact du Règlement général sur la protection des données dans le secteur de la santé » du présent ouvrage.

§ 6. Traitement aux fins de médecine préventive ou médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale

30. Cette exception reprise à l'article 9, § 2, h), englobe un pan entier de la médecine allant de la prévention à la surveillance du travailleur par le biais de l'appréciation de la capacité de travail dudit travailleur.

En effet, le médecin du travail se déplaçant chez l'employé afin de vérifier s'il se trouve réellement en incapacité de travail effectuera une évaluation de sa capacité de travail et se trouvera donc dans le champ d'application de cette exception impliquant également le respect des législations nationale ainsi que des principes de minimisation et de nécessité. À noter que l'employeur ne peut, en aucun cas, se prévaloir de cette exception.

Les experts techniques pourraient également entrer dans ce champ d'application à considérer qu'ils puissent revêtir la qualification de responsable de traitement, aspect qui est analysé dans le chapitre consacré à « l'impact du Règlement général sur la protection des données dans le secteur de la santé » du présent ouvrage.

31. L'article 9, § 2, h), impose une condition complémentaire à charge des responsables du traitement. En effet, le traitement des données à caractère personnel peut uniquement être effectué « par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents »⁶².

La formulation de cette obligation est légèrement différente de celle donnée par la directive 95/46/CE en ce qu'elle étend les personnes habilitées à bénéficier de cette exception aux personnes travaillant sous sa responsabilité. Cependant, le RGPD ne précise pas la notion que recouvre le terme de responsabilité. S'agit-il de la notion de responsabilité civile ou hiérarchique ou même organisationnelle ? Il nous paraît logique de considérer que nous nous situons plus sous l'angle hiérarchique ou organisationnel en lien avec la qualité des données traitées qui doit être assurée, compte tenu du fait que le RGPD consacre l'article 82 à la responsabilité de dommage.

Même si l'on ne cerne pas clairement ce qu'il faut entendre par « sous sa responsabilité » on comprend que la loi impose l'intervention d'un tel professionnel chaque fois que des données sont traitées et que « le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé ».

32. L'on doit également noter que le RGPD ne définit pas la notion de « professionnel de la santé », ce qui permet de considérer qu'il renvoie au droit national, en ce compris les conditions d'accès à la profession, à défaut d'une qualification au niveau européen via, par exemple, la Cour de justice de l'Union européenne. Ainsi que le relève Céline Roynier, « la comparaison des définitions des différentes professions de santé dans les législations de [diverses législations européennes] montre que trois composantes y sont systématiquement articulées »⁶³, à savoir la qualification, l'objet du travail et les missions du système de santé. Au niveau belge, l'on peut renvoyer à l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions des soins de santé.

⁶² Art. 9, 3, du RGPD.

⁶³ C. ROYNIER, « les Professionnels de santé en Europe : contribution à une définition unitaire », *Les Tribunes de la santé*, 2015/3 (n° 48), pp. 34-35.

SECTION 3. – L'article 10 du RGPD

33. Si une première lecture de d'article 10 du RGPD laisse à penser qu'il s'agit d'une copie conforme de l'article 8.5 de la directive 95/46/CE, cela n'est pas totalement exact. En effet, le présent article 10 ne concerne que les seules données liées aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, du RGPD sans plus pouvoir être étendu aux sanctions administratives, ou aux jugements civils. L'on voit donc que le champ d'application est réduit et que la marge de manœuvre des États membres pour élargir la notion de données judiciaires a été réduite à néant.

Au niveau de la détermination des personnes et autorités pouvant traiter les données visées à l'article 10, le RGPD renvoie aux législations nationales⁶⁴.

L'on doit également relever que la directive 2016/680/UE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil a pour objectif d' « établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »⁶⁵.

Dans le cadre de la présente contribution, nous n'allons pas approfondir ces aspects dès lors que cela est analysé dans la contributions intitulée « La protection des données dans les secteurs de la "police" et de la "justice" » du présent ouvrage.

⁶⁴ Voy. art. 10 de la loi du 19 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel soumise à la sanction royale ; art. 9 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2018-493 du 20 juin 2018.

⁶⁵ Art. 1^{er} de la directive 2016/680/UE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Conclusion

34. Si l'on peut se réjouir de constater que le RGPD ne modifie pas les principes essentiels de la protection des données à caractère personnel, il est cependant regrettable que le législateur européen n'en ait pas profité pour « mettre à plat » certains concepts tels que les données particulières pour supprimer les ambiguïtés que l'article 9 continue à véhiculer ainsi que nous l'avons vu ci-dessus.

Il eût été utile d'introduire de manière claire la notion de contexte dans lequel les données sont traitées pour éviter des situations dans lesquelles une donnée particulière est effectivement traitée mais pas pour son caractère particulier. Ainsi, l'utilisation d'une photo d'une personne portant un signe religieux pour un annuaire repris sur le site Internet d'une société constitue-t-elle un traitement de donnée particulière alors que le responsable de traitement n'a pas égard à la religion mais uniquement à l'identification de la personne comme employée de la société ? Répondre à cette question impose une gymnastique délicate qui aurait pu être évitée si le législateur européen avait veillé à contextualiser le caractère particulier des données.

35. La particularité du RGPD réside dans le fait qu'il est en réalité un moyen terme entre un règlement et une directive en ce qu'il laisse des marges de manœuvre pour les États membres. Or, ces marges de manœuvre peuvent mettre à mal le principe de cohérence européenne qui est précisément visé par ce même RGPD. Cherchez l'erreur !

Cependant, et heureusement osons-nous dire, le RGPD rappelle et précise des principes uniques pour l'ensemble des États membres et crée un réel territoire de libre circulation des données amenant un meilleur contrôle de ses données par les individus quelle que soit leur nationalité. En effet, il ne faut pas perdre de vue que l'Union européenne est une union économique et que le RGPD a, pour objectif premier, de permettre une libre circulation des données avec ce qu'elle a d'économique tout en prodiguant une protection des données nécessaires à une telle circulation.