Le big data en matière d'assurances à l'épreuve du RGPD

Jacquemin, Hervé; Van Gyseghem, Jean-Marc

Published in:
Dara protection

Publication date:
2017

Document Version
le PDF de l'éditeur

Le big data en matière d'assurances à l'épreuve du RGPD

Hervé JACQUEMIN
Chargé de cours à l'Université de Namur (CRIDS)
Avocat au barreau de Bruxelles

Jean-Marc VAN GYSEGHEM
Directeur de recherches au CRIDS
Avocat au barreau de Bruxelles

SAMENVATTING

Big data – laat er geen twijfel over bestaan – vormen een belangrijke potentiële informatiebron voor verschillende economische actoren, waaronder de verzekeringsondernemingen. Behalve het feit dat de big data hen meer kennis over hun klanten verschaffen, met name voor marketingdoeleinden, zal de exploitatie van de gegevens afkomstig van big data de beoordeling van de te verzekeren risico's vergemakkelijken. Men stelt overigens vast dat door het steeds stijgende gebruik van het Internet of things (IoT) – in de vorm van geconnecteerde toepassingen aan boord van voertuigen of die geïntegreerd zijn in alledaagse voorwerpen (geconnecteerde uurwerken bijvoorbeeld) – de hoeveelheid gegevens die de verzekeraars kunnen verzamelen en verwerken, exponentieel stijgt.

Vanzelfsprekend zijn aan dit fenomeen een aantal belangrijke zaken verbonden zoals de bescherming van de persoonlijke levenssfeer en de verwerking van persoonsgegevens.

Deze bijdrage maakt hiervan een analyse, tegen de achtergrond van de nieuwe Algemene Verordening betreffende de bescherming van persoonsgegevens (GDPR). Er moet immers zekerheid zijn dat de verwerking van gegevens door de verzekeraars conform de in de Verordening opgenomen beginselen gebeurt, in het bijzonder de beginselen rond doelbinding, minimale gegevensverwerking en juistheid. We bekijken daarnaast de rechtmatigheid van de verwerking, die samenhangt met de toestemming van de verzekerde, maar ook diens rechten in het licht van een verwerking, die vaak wel discreet gebeurt door de verzekeraar, maar belangrijke juridische gevolgen meebrengt voor die verzekerde. Het belang hiervan kan niet onderschat worden gelet op het feit dat sommige beslissingen automatisch genomen zouden kunnen worden.

Alle facetten van deze problematiek worden aldus onderzocht doorheen de verschillende fases die een verzekeringsovereenkomst doorloopt, dit zijn de sluiting, de vaststelling van het risico en van de premie, het beheer na een schadegeval enz.

RÉSUMÉ

Le big data est, à n'en pas douter, une source d'information potentielle importante pour divers acteurs économiques au nombre desquels l'on retrouve les compagnies d'assurances. En effet, outre qu'il leur permet de mieux connaître leurs clients, à des fins de marketing notamment, l'exploitation des données issues du big data facilitera l'évaluation des risques à assurer. On observe d'ailleurs qu'avec le recours croissant à l'Internet des objets (IoT) – sous la forme d'applications connectées embarquées dans les véhicules ou intégrées aux objets de tous les jours (montres connectées, par exemple) – les données susceptibles d'être collectées et traitées utilement par les assureurs augmentent de façon exponentielle.

On conçoit sans peine que le phénomène pose des enjeux majeurs en termes de protection de la vie privée et de traitement des données à caractère personnel.

La présente contribution analyse ceux-ci, à l'aune des dispositions du nouveau Règlement général relatif à la protection des données à caractère personnel (RGPD ou GDPR). Il faut en effet s'assurer que les traitements envisagés par les assureurs sont conformes aux principes consacrés par le Règlement, en particulier les principes de

limitation des finalités, de minimisation des données et d'exactitude. On se penche aussi sur la question de la licéité du traitement, en lien avec le consentement de l'assuré mais aussi de ses droits au regard d'un traitement qui est bien souvent discret mais créateur d'effets juridiques importants pour ce même assuré. C'est d'autant plus crucial que certaines décisions pourraient être prises de manière automatisée.

Les enjeux posés par la problématique sont ainsi examinés au travers des diverses étapes de la vie d'un contrat d'assurance, à savoir la conclusion, la détermination du risque et de la prime, la gestion en cas de sinistre, etc.

I. Quelles utilisations possibles du big data dans le secteur des assurances?

1. Le phénomène du « big data ». Avec le développement croissant des technologies de l'information et de la communication, qui allient une capacité de stockage en augmentation constante, notamment dans le Cloud, et une infrastructure technique permettant d'échanger les données rapidement et en grand volume, les conditions techniques sont satisfaites pour mettre une quantité exponentielle de données, structurées ou non, à la disposition des entreprises – spécialement les GAFA (1) – ou des autorités publiques. Parallèlement et à mesure que les capacités techniques s'améliorent, leur prix tend à diminuer.

On parle ainsi de « big data » ou, en français, de « données massives » ou de « mégadonnées » (2).

Les sources de ces données sont nombreuses et variées. Elles peuvent être fournies par les utilisateurs eux-mêmes ou les entreprises, volontairement ou pas, sciemment ou pas, à travers par exemple les réseaux sociaux, les sites Internet transactionnels ou de partage de contenus ainsi que les jeux en ligne. En réalité, toute trace laissée à l'occasion d'une activité sur l'Internet ou à travers une application dédiée, sur son appareil mobile, constitue une donnée: l'historique de navigation ou une simple recherche dans Google peuvent ainsi fournir des informations intéressantes dans le cadre du big data.

(1) Acronyme qui désigne Google, Apple, Facebook et Amazon, soit quatre des plus puissantes entreprises du monde de l'Internet.

(2) Pour une description du phénomène et de ses principales caractéristiques, voy. V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data – La révolution des données est en marche,* Paris, Ed. Robert Laffont, 2014; A. LATREILLE et C. ZOLYNSKY, « Séance 4: nouvelles pratiques: faut-il de nouvelles protections? », *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Expert*, Paris, Société de Législation comparée, 2014, pp. 262 et s.; M. MAIRLOT, « Big Data et vie privée: mariage possible? », *Dr. Banc. Fin.*, 2015/VI, p. 446; A. GROSJEAN, « Le profilage: un défi pour la protection des données à caractère personnel », *Enjeux européens et mondiaux de la protection des données personnelles,* Bruxelles, Larcier, 2015, n° 17 et s.; P. DE FILIPPI, « Gouvernance algorithmique: vie privée et autonomie individuelle à l'ère des Big Data », *Open Data & Big Data – Nouveaux défis pour la vie privée,* Paris, Mare & Martin, 2016, pp. 99 et s.; E. LUTS, « Big data in de financiële sector », *Rev. Banc. Fin.*, 2016/2, pp. 123 et s. Voy. aussi Groupe 29, « Opinion 03/2013 on purpose limitation », WP203, 2 avril 2013, p. 35 et pp. 45 et s.

Ce volume tend à s'accroître davantage encore grâce aux données collectées par les objets connectés – on parle d'Internet des objets ou IoT (3) – qui se multiplient, et qui fournissent, souvent en temps réel, des informations nombreuses et variées, par exemple en termes de géolocalisation: on pense par exemple aux montres connectées, aux applications de domotique ou aux véhicules automobiles.

Enfin, l'existence de données publiques – open data – mises à la disposition de tous est une autre explication du succès des big data.

Ce volume considérable de données ne présente de l'intérêt que s'il est possible de l'analyser efficacement, pour en tirer des enseignements utiles, notamment en termes prédictifs. Comme certains l'indiquent pertinemment, il s'agit de « laisser parler les données » (4). Les progrès techniques permettent d'atteindre cet objectif, au moyen d'algorithmes de plus en plus sophistiqués, qui livrent des résultats généraux (en identifiant certaines tendances sur le marché, par exemple), ou plus précis (en procédant par exemple au profilage des personnes, de manière à leur appliquer des décisions automatisées). Comme l'a écrit le Contrôleur européen de protection des données, « l'une des utilisations potentiellement les plus importantes des données massives est de prédire ce qui va probablement se produire, mais ne s'est pas encore produit, et ce que nous allons probablement faire, mais n'avons pas encore fait » (5).

Pour circonscrire et expliquer le phénomène du big data, on fait traditionnellement référence aux trois V (6). Ils désignent le Volume massif de données – et en croissance exponentielle – à la disposition de certaines entreprises; leur Variété, puisqu'il peut s'agir de données à caractère personnel ou d'autres catégories d'informations, structurées ou pas, et sous des formats divers (texte, image, son, etc.) et la Vitesse à laquelle il est maintenant possible de les collecter et de les traiter, en temps réel dans certains cas.

(3) Voy. à ce sujet Groupe 29, « Avis 8/2014 sur les récentes évolutions relatives à l'Internet des objets », WP223, 16 septembre 2014; C. BRION, H. WAEM et Y. HENDRICKS, « The Big Cloud of Things is watching you: le droit de la vie privée et l'Internet des objets », *La révolution digitale et les start-ups,* Brxuelles, Larcier, 2016, pp. 213 et s.; Voir, entre autres, communiqué de presse de la Commission européenne du 19 avril 2016 et la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 avril 2016, COM (2017)/76 final; Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, "Créer une économie européenne fondée sur les données", COM (2017)/9 final.

(4) V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data – La révolution des données est en marche,* Paris, Ed. Robert Laffont, 2014, pp. 14 et s.; A. LATREILLE et C. ZOLYNSKY, « Séance 4: nouvelles pratiques: faut-il de nouvelles protections? », *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Expert*, Paris, Société de Législation comparée, 2014, p. 265.

(5) EDPS, « Relever les défis des données massives », Avis n° 7/2015, 19 novembre 2015, p. 9.

(6) P. DE FILIPPI, « Gouvernance algorithmique: vie privée et autonomie individuelle à l'ère des Big Data », *Open Data & Big Data – Nouveaux défis pour la vie privée,* Paris, Mare & Martin, 2016, pp. 99 et s.; A. LATREILLE et C. ZOLYNSKY, « Séance 4: nouvelles pratiques: faut-il de nouvelles protections? », *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Expert*, Paris, Société de Législation comparée, 2014, p. 263; C. BRION, H. WAEM et Y. HENDRICKS, « The Big Cloud of Things is watching you: le droit de la vie privée et l'Internet des objets », *La révolution digitale et les start-ups,* Bruxelles, Larcier, 2016, pp. 233-234.

On pourrait y ajouter un V supplémentaire, relatif à la Valeur de ces données (7), spécialement s'il s'agit de données à caractère personnel. Elles constituent d'ailleurs l'un des éléments-clés de notre économie numérique, au point que l'on peut parler d'« économie de la donnée ». Il est ainsi intéressant de constater que, dans une Proposition récente de directive de la Commission concernant certains aspects des contrats de fourniture de contenus numériques (8), il est expressément prévu que le texte « s'applique à tout contrat par lequel un fournisseur fournit un contenu numérique au consommateur ou s'engage à le faire, en échange duquel un prix doit être acquitté ou une *contrepartie non pécuniaire, sous la forme de données personnelles ou de toutes autres données*, doit être apportée de façon active par le consommateur » (9). On place ainsi les données à caractère personnel ou d'autres données sur le même pied que le paiement d'un prix en contrepartie de la fourniture de contenus numériques.

2. Big data et assurances. Dans le domaine des assurances, comme dans de nombreux autres secteurs d'activités, les entreprises sont soucieuses de tirer le meilleur parti des données à leur disposition. Nombre d'entre elles disposent déjà, en interne, d'un volume important de données, qui peut leur être utile moyennant l'application d'algorithmes correctement configurés. Elles sont en outre intéressées d'enrichir cette base de données, à l'aide d'autres données disponibles librement et publiquement, de données acquises auprès de tiers, ou d'objets connectés utilisés par les personnes concernées.

Ces données tirées du big data présentent de l'intérêt à tous les stades de la vie d'un contrat d'assurance (en ce compris au stade précontractuel) (10). Peu importe, du reste, qu'il s'agisse d'assurances de personnes (une assurance-vie, par exemple) ou de dommage (une assurance habitation ou RC auto, par exemple).

En termes de marketing, il est évidemment utile d'anticiper, en termes prédictifs, les attentes du marché pour proposer rapidement – et si possible avant les concurrents – des produits qui répondent adéquatement aux besoins des prospects ou des clients. De même, en combinant les informations recueillies au moyen de cookies installés sur les terminaux des consommateurs, avec d'autres informations qui les concernent, des publicités ciblées et personnalisées, pour certains produits d'assurances, peuvent leur être envoyées.

Avant de conclure un contrat avec un preneur, la compagnie d'assurances souhaite disposer d'autant d'informations que possible, pour évaluer le risque au mieux (et refuser, le cas échéant, de le couvrir) et calculer la tarification. La compagnie pourrait ainsi être intéressée de connaître l'état de santé de son assuré, avant de le couvrir en vie ou en soins de santé, par exemple au moyen des données de santé collectées – volontairement ou à son insu – par son smartphone ou sa montre intelligente. Le big data pourrait d'ailleurs permettre d'identifier les risques de santé, sans

(7) A. LATREILLE et C. ZOLYNSKY, « Séance 4: nouvelles pratiques: faut-il de nouvelles protections? », *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Expert*, Paris, Société de Législation comparée, 2014, p. 263.

(8) Proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture de contenus numériques, COM(2015) 634 final.

(9) C'est nous qui soulignons.

(10) Pour des illustrations, voy. P. DE FILIPPI, « Gouvernance algorithmique: vie privée et autonomie individuelle à l'ère des Big Data », *Open Data & Big Data – Nouveaux défis pour la vie privée*, Paris, Mare & Martin, 2016, p. 112.

collecter, en tant que telles, ces données (par le biais d'une prise de sang, par exemple): un modèle prédictif a ainsi été élaboré pour identifier les personnes présentant un plus grand risque d'être victimes d'hypertension artérielle ou de diabète. Il se base sur des données « concernant le style de vie et comparant des centaines de variables relatives aux loisirs, à la visite de tel ou tel site Web, au nombre d'heures passées devant la télévision ainsi que l'estimation du revenu » (11).

C'est dans ce contexte également que le système de tarification « *pay how you drive* » commence à être testé et diffusé (12): il s'agit plus précisément de calculer la prime en fonction de la conduite de l'assuré, dont tous les paramètres sont précisément collectés et analysés au moyen d'objets connectés présents dans le véhicule. On bascule ainsi d'un modèle qui se nourrit des informations générales transmises par l'assuré, et complété par des statistiques, à un examen en temps réel (ou presque) extrêmement précis, qui permet d'individualiser la prime pour chacun. Pour de jeunes « bons » conducteurs, cela permet d'obtenir une réduction des primes.

De même, en matière d'assurance RC habitation, la compagnie pourrait juger pertinent de savoir, par exemple à l'occasion d'informations diffusées sur Facebook ou d'autres sources, que le quartier dans lequel l'immeuble est situé fait régulièrement l'objet de cambriolages. L'analyse des risques d'inondation pourrait également s'enrichir des modèles météorologiques disponibles pour telle ou telle région, couplés à un examen cartographique précis du sol, disponibles en open data, de manière à moduler la prime en fonction du risque (ce qui, du reste, se fait déjà en partie).

Enfin, en cas de sinistre, la compagnie d'assurances sera intéressée de connaître les informations susceptibles d'être fournies par les objets connectés. Ainsi, certains véhicules automobiles collectent en permanence des données sur la localisation du véhicule, le mode de conduite et son caractère plus ou moins sportif, la vitesse, les variations de trajectoire, etc. Elles peuvent être transmises au constructeur en temps réel, les véhicules étant équipés d'une carte SIM, ou lors d'une visite au garage. À la suite d'un accident, la compagnie peut ainsi être intéressée de savoir que le trajet a commencé à l'adresse d'un bar à vin, et qu'avant l'accident, le conducteur avait conduit à une vitesse excessive, en mobilisant à de nombreuses reprises certains équipements de sécurité à sa disposition (alarme anticollision ou croisement de lignes blanches, par exemple).

Des algorithmes sophistiqués peuvent encore faciliter l'identification des fraudes éventuellement commises par certains assurés, par exemple en incendie, ce qui peut inciter la compagnie à envoyer un expert pour contrôler les déclarations des clients et vérifier l'étendue réelle du dommage.

En définitive, dans le domaine des assurances, les opportunités offertes par le big data sont extrêmement nombreuses, et devraient d'ailleurs se multiplier à l'avenir, à mesure que la masse de données augmente, ainsi que l'efficacité des algorithmes chargés de les « faire parler ». Le phénomène est loin d'être anodin et pourrait révolutionner le métier, avec une individualisation extrêmement précise des risques assurés, et des primes corrélatives.

(11) V. MAYER-SCHÖNBERGER et K. CUKIER, *Big Data – La révolution des données est en marche*, Paris, Ed. Robert Laffont, 2014, p. 73.

(12) A ce sujet, voir V. VERBRUGGEN, *Ma voiture, (encore et toujours) ma liberté? L'assurance "Payez comme vous conduisez": "ultrapersonnalisation" du risque et risque d'atteinte à la vie privée et à la protection des données personnelles"*, Forum de l'assurance, 2017, nr.173, p. 75 et s.

3. Risques et enjeux du big data – les réponses du RGPD? Le big data présente des avantages indéniables, à titre individuel et collectif: on pense aux progrès susceptibles d'être engrangés dans le domaine de la recherche médicale, de la prévention de certaines épidémies ou de catastrophes naturelles, ainsi qu'en matière de détection des fraudes (13).

Malheureusement, ces forces sont souvent éclipsées par les risques tout aussi indéniables posés par le big data. Lorsque des données à caractère personnel sont concernées (ce qui sera souvent le cas), on peut en effet craindre que le traitement réalisé porte atteinte à la vie privée des individus (14) et que des choix discriminatoires, illégitimes ou injustes soient posés sur cette base. Ce sera plus particulièrement le cas lorsque des décisions sont prises, en termes d'assurabilité ou de calcul des primes, sur la base des informations tirées des big data analysées (15). On peut craindre en effet que certaines personnes soient finalement exclues du marché normal de l'assurance, ou doivent payer des primes particulièrement élevées.

Le risque existe également d'un certain conformisme, auquel les personnes pourraient être tentées de se soumettre, pour être en phase avec les critères dégagés d'une analyse big data (correspondant par exemple à ce que fait le plus grand nombre et qu'un algorithme a désigné comme étant la norme à suivre) et, ainsi, bénéficier de conditions tarifaires plus réduites (16). Ce faisant, on brise les velléités d'innovation ou de choix différents, guidés par la liberté individuelle et le libre arbitre, qui pourraient pourtant être sources de progrès.

De manière plus générale, le big data pose d'évidentes questions de nature philosophique ou éthique, puisqu'on accepte désormais d'être gouverné par les données et les algorithmes chargés de leur donner sens. Dans la présente contribution, il nous est malheureusement difficile de développer ce point.

(13) Voy. not. la Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Vers une économie de la donnée prospère », COM(2014) 442 final.

(14) Pointant certains risques du big data en termes de vie privée et de traitement des données à caractère personnel, voy. M. MAIRLOT, « Big Data et vie privée: mariage possible? », *Dr. Banc. Fin.*, 2015/VI, pp. 448 et s.; P. DE FILIPPI, « Gouvernance algorithmique: vie privée et autonomie individuelle à l'ère des Big Data », *Open Data & Big Data – Nouveaux défis pour la vie privée,* Paris, Mare & Martin, 2016, pp. 104 et s.; L. MERLAND, « L'identité civile des personnes: Is big data beautiful? », *R.L.D.I.*, 2015/121, pp. 37 et s. Voy. aussi Groupe 29, « Opinion 03/2013 on purpose limitation », WP203, 2 avril 2013, p. 35 et pp. 45 et s.; EDPS, « Relever les défis des données massives », Avis n° 7/2015, 19 novembre 2015, pp. 8 et s.

(15) Antoine LATREILLE et Célia ZOLYNSKI signalent, à juste titre, que l'usage du big data « transforme le 'déluge de data' analysées en information voire en outil de décision ». (A. LATREILLE et C. ZOLYNSKI, « Nouvelles pratiques: faut-il de nouvelles protections? », *in La proposition de Règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Experts*, Collection Trans Europe Experts, vol. 9, p. 264).

(16) Voy. en ce sens EDPS, « Relever les défis des données massives », Avis n° 7/2015, 19 novembre 2015, p. 10: « la nécessité d'obtenir un prêt ou une couverture d'assurance pourrait pousser ou contraindre des individus à éviter le contact avec certaines personnes ou entreprises ou à visiter des quartiers où les taux de criminalité sont élevés de la même manière que des personnes sont incitées à installer des 'boîtes noires' qui permettent à un responsable de traitement externe de les contrôler pendant qu'elles conduisent ».

On se concentre sur la conformité du recours au big data dans le domaine des assurances, à l'aune du nouveau régime instauré par le Règlement général de protection des données (17) (ci-après, « RGPD » ou « Règlement »), applicable à partir du 25 mai 2018. Sauf exception, nous ne ferons pas de référence systématique aux dispositions de la directive 95/46/CE (18) ou à celles 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, qui la transpose en droit belge (ci-après, LVP) qui sont toutes deux vouées à disparaître au profit du Règlement.

4. Plan et limites de la présente contribution. D'autres articles du présent *Dossier* analysent déjà, de manière détaillée, le régime introduit par le RGPD. Dans la présente contribution, nous nous limitons aux aspects susceptibles de poser des difficultés dans le domaine du big data.

Nous examinons d'abord le phénomène du big data à la lumière des principes consacrés à l'article 5 du RGPD et qui s'appliquent à tout traitement de données (limitation des finalités, minimisation des données, exactitude, etc.). On analyse ensuite les bases de légitimation susceptibles d'assurer la licéité du traitement, en insistant particulièrement sur le consentement de la personne concernée, dont les exigences ont été renforcées par le RGPD. Les droits de la personne concernée sont ensuite présentés.

II. Le big data à l'aune des principes directeurs consacrés par le Règlement

5. Les intervenants. Il est important de déterminer les fonctions de chaque acteur du traitement telles qu'analysées au regard du Règlement. Pour rappel, il est ici question de traitement effectué par des compagnies d'assurances en utilisant le big data pour, par exemple, procéder à une analyse de risques d'un client présent ou à venir.

Pour ce faire, cette compagnie peut collecter des informations, soit auprès de son client, soit auprès de tiers, pour une utilisation qui n'était généralement pas envisagée dans le traitement initial.

Il peut ainsi s'agir d'un traitement ultérieur dès lors que les informations proviennent d'un responsable de traitement initial qui a collecté des données pour son propre traitement. Ensuite, ces données sont communiquées à une compagnie d'assurances pour un nouveau traitement consistant en l'analyse du risque, par exemple.

(17) 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 (règlement général sur la protection des données), *J.O.*, 4 mai 2016, n° L.119. Pour une première analyse du Règlement, voy. C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016/62, pp. 5 et s.; E. DEGRAVE, « La protection des données à caractère personnel enfin réformée », *J.D.E.*, 2016, pp. 136 et s.; *Data protection & Privacy – Le GDPR dans la pratique/De GDPR in de praktijk*, Limal, Anthemis, 2017, 230 p. Voy. également le commentaire article par article réalisé par Th. LÉONARD et D. CHAUMONT et disponible sur le site www.GDPR-expert.eu.

(18) 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.

Ce concept de « traitement ultérieur » sera présenté de manière plus approfondie ci-après.

Quelle que soit l'hypothèse, il faudra déterminer le statut de la compagnie d'assurances au regard du RGPD et de la définition qu'il donne du responsable de traitement (19). À la question de la détermination des finalités, il ne fait aucun doute que la réponse doit être positive dès lors que la compagnie d'assurances détermine l'objectif qu'elle entend poursuivre en traitant les données. Par ailleurs, elle procédera également à la détermination des moyens à mettre en œuvre pour ce faire, à savoir l'utilisation de données récoltées soit directement auprès du client soit auprès de tiers.

Rien n'empêche, par ailleurs, que d'autres personnes soient appelées à intervenir, soit comme sous-traitant de la compagnie d'assurances, soit comme co-responsable, en fonction des hypothèses rencontrées.

Quant à la personne concernée, il s'agira du preneur d'assurance, de l'assuré ou du demandeur de contrat d'assurance.

6. Principes applicables à tout traitement de données à caractère personnel. L'article 5 du RGPD énonce les principes auxquels est soumis tout traitement de données à caractère personnel: licéité, loyauté et transparence; limitation des finalités, minimisation des données; exactitude; limitation de la conservation; intégrité et confidentialité; responsabilité. D'autres dispositions du Règlement complètent ou précisent certains de ces principes (voy. p. ex. art. 12 et s., qui établissent les droits de la personnes concernée en matière de transparence).

Ces principes étaient déjà consacrés par la directive 95/46/CE et la LVP et, pour l'essentiel, le Règlement les reprend sans modification majeure. On peut cependant noter des différences, ici ou là (20).

Il incombe à tout responsable du traitement (une compagnie d'assurances, par exemple) de vérifier, au cas par cas et avant de lancer un projet fondé sur des résultats big data, si ces principes sont dûment respectés en l'espèce. Cette démarche préalable et systématique est indispensable.

Elle est toutefois loin d'être facile, ne serait-ce qu'en raison de la distinction à opérer entre la collecte initiale des données et les traitements, ultérieurs ou non, opérés à l'aide des algorithmes en vue de donner un sens utile aux données dont on dispose. Dans un certain nombre de cas, la compagnie d'assurances voudra utiliser des données qu'elle n'a pas collectées elle-même et qui ont été obtenues pour des finalités qui peuvent être totalement différentes. L'intérêt du big data consiste en effet à faire parler les données, au point de leur donner, dans certains cas, un sens distinct (avec un effet prédictif).

(19) Art. 4, 7°, du Règlement: « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

(20) À ce sujet, voy. C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, *o.c.*, pp. 18 et s.

La pluralité d'intervenants est aussi source de complexité. On songe notamment aux données de conduite collectées par les objets connectés présents dans un véhicule automobile, lors d'un accident de la circulation. Le responsable du traitement est généralement le constructeur du véhicule. La compagnie d'assurances n'a, quant à elle, pas forcément de relation contractuelle directe avec le conducteur, par exemple en cas de leasing du véhicule. On peut certes imaginer que le traitement initial de collecte a fait l'objet d'une analyse de conformité au RGPD par le responsable concerné. Il est toutefois recommandé à la compagnie d'assurances, qui intervient en aval, de prendre les garanties contractuelles qui s'imposent vis-à-vis du fournisseur de données, de sorte qu'il prenne la responsabilité de l'anonymisation des données (pour sortir du champ d'application du RGPD) ou du respect des principes de licéité consacrés par le Règlement.

En matière de big data, comme pour tout traitement de données à caractère personnel, chacun de ces principes est important et doit être scrupuleusement respecté par le responsable du traitement.

Nous les examinons successivement, à l'exception du principe de licéité, transparence et loyauté, visé sous le point III de la présente contribution, et du principe d'intégrité et de confidentialité (21), qui ne pose pas de question spécifique en matière de big data. Préalablement, il importe de rappeler que ces principes ne s'appliquent qu'aux données à caractère personnel, à l'exclusion, notamment des données anonymisées (à ne pas confondre avec les données pseudonymisées qui, elles, sont des données à caractère personnel).

7. Données à caractère personnel, anomymisation et pseudonymisation. Les données à caractère personnel sont définies à l'article 4, 1°, du Règlement comme « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée 'personne concernée'); est réputée être une 'personne physique identifiable' une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». De nombreuses données issues du big data que les compagnies d'assurances pourraient vouloir utiliser répondent à cette définition.

Pour échapper aux exigences prescrites par le Règlement, la solution peut consister à anonymiser les données. Encore faut-il que la personne concernée ne soit plus identifiable de manière irréversible, ce qui pourrait faire l'objet de discussions. Le considérant n° 26 du Règlement apporte des précisions sur ce point: aux termes de celui-ci, « 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 identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci ».

(21) Art. 5, § 1er, f), du Règlement.

Dans le contexte du big data, où le volume des données susceptible d'être utilisé est particulièrement important, le risque d'une possible (ré)-identification de la personne concernée augmente corrélativement (22). Aussi sera-t-on très attentif au moment de décider si les données peuvent être considérées comme étant « anonymes »: la qualification est délicate pour les traitements traditionnels, et davantage encore en matière de big data (23); s'il apparaît ultérieurement que les données ne sont pas anonymes, parce qu'une personne physique peut être identifiée ne fut-ce qu'indirectement, il faudra gérer *a posteriori* un traitement pour lequel aucune mesure n'a été prise en vue d'en assurer la licéité (aucun consentement préalable n'ayant été obtenu de la personne concernée, par exemple), ce qui exposera très probablement l'entreprise concernée à une lourde sanction de la part des autorités de contrôle.

Le Règlement reste par contre applicable aux données pseudonymisées: la pseudonymisation est définie comme « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable » (art. 4, 5°, du Règlement). En recourant à ce type de mesure, qui réduit sensiblement les risques auxquels sont exposées les personnes concernées en termes de protection de leurs données à caractère personnel, le responsable du traitement pourra plus facilement démontrer qu'il respecte les obligations qui lui incombent conformément au RGPD. On verra en effet que c'est l'un des éléments à prendre en considération au moment de déterminer si un traitement ultérieur est compatible avec les finalités initiales (*infra*). Aussi faut-il encourager les parties prenantes à recourir à cette méthode, dans la mesure permise par les traitements qu'ils envisagent.

8. Principe de limitation des finalités. Conformément à l'article 5, § 1er, b), du Règlement, les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1er, comme incompatible avec les finalités initiales ».

(22) C. BRION, H. WAEM et Y. HENDRICKS, « The Big Cloud of Things is watching you: le droit de la vie privée et l'Internet des objets », *La révolution digitale et les start-ups,* Bruxelles, Larcier, 2016, pp. 234: « l'anonymisation ne semble toutefois pas être une véritable solution dans un contexte de big data ».

(23) En ce sens, voy. A. LATREILLE et C. ZOLYNSKY, « Séance 4: nouvelles pratiques: faut-il de nouvelles protections? », *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe Expert*, Paris, Société de Législation comparée, 2014, p. 267: « la puissance des pratiques 'big data' pourrait faire qu'un traitement de données à caractère personnel soit possible alors que, prises isolément, chaque base ne contient pas de données à caractère personnel. Le traitement 'big data' peut, par croisement, conduire à des pratiques de ré-identification, notamment par le biais de techniques de zoomage permettant de passer du 'big' à la 'nano', et ainsi de faire parler ces données non identifiantes à des fins d'identification des personnes. [...] Nombreux considèrent alors, avec les possibilités de croisements et la logique du recoupement du traitement Big Data, que les pratiques d'anonymisation actuelle ne sauraient être efficaces ».

Il s'agit d'un principe fondamental en matière de protection des données: la personne concernée doit savoir à quelle fin ses données sont collectées par le responsable du traitement. Aussi lui incombe-t-il à ce dernier, par application du principe de transparence, d'informer la personne concernée sur ce point. En pratique, cet élément figurera généralement dans la politique de confidentialité ou tout autre document contractuel fourni à la personne concernée. Il faut par ailleurs s'assurer que celui-ci lui soit opposable.

Dans le domaine du big data, la question du traitement ultérieur compatible avec les finalités initiales ne manquera pas de se poser. L'objectif est en effet d'exploiter utilement le volume important des données dont on dispose pour en tirer des enseignements sur la personne concernée, à des fins de marketing ou pour cerner plus précisément son profil de risque. Or, pour la plupart, ces données n'ont pas forcément été collectées à cette fin. La situation se complique encore sachant que les données ont pu être collectées initialement par un autre responsable de traitement, qui se ménagerait le droit de les communiquer à des tiers (en l'occurrence, la compagnie d'assurances).

L'analyse est assurément complexe et, pour faciliter la tâche de l'interprète chargé de le mettre en œuvre, le Règlement énonce les principes à prendre en considération pour procéder à l'évaluation. Sans que la liste soit limitative, on peut ainsi tenir compte, aux termes de l'article 6, § 4, du Règlement, « a) de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé; b) du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement; c) de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, en vertu de l'article 9, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 10; d) des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées.

Lorsqu'il s'agit, pour la compagnie d'assurances, de traiter des données de santé – les activités physiques et la fréquence cardiaque – collectées par la montre connectée de la personne concernée en vue d'évaluer le risque avant de la couvrir en soins de santé, on peut sérieusement douter que cette finalité soit compatible avec le point c) de l'article 6, § 4, précité.

Même si le responsable ne parvient pas à démontrer que le traitement ultérieur est compatible avec les finalités initiales, celui-ci ne sera pas nécessairement interdit. Le Règlement confirme en effet clairement – et c'est une nouveauté – qu'un traitement ultérieur pour des finalités incompatibles avec les finalités initiales est permis, moyennant le respect de certaines conditions.

L'article 6, § 4, du Règlement l'autorise dans deux hypothèses: lorsqu'il est fondé sur « le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre qui constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir les objectifs visés à l'article 23, § 1er ».

À cet égard, on doit se rappeler que, suivant la Proposition introduite par la Commission en janvier 2012, l'autorisation des traitements ultérieurs incompatibles avec les finalités initiales était admise beaucoup plus largement: l'article 6, § 4, de

la Proposition indiquait en effet que « lorsque la finalité du traitement ultérieur n'est pas compatible avec celle pour laquelle les données à caractère personnel ont été collectées le traitement doit trouver sa base juridique au moins dans l'un des motifs mentionnés au paragraphe 1er, points a) à e). Ceci s'applique en particulier à toute modification des clauses et des conditions générales d'un contrat ». Plusieurs conditions de licéité – et pas seulement le consentement de la personne concernée – pouvaient donc être invoquées pour autoriser le traitement ultérieur. Dans la Proposition de la Commission, seul l'intérêt légitime du responsable du traitement ou d'un tiers ne pouvait pas être invoqué (*cf.* littera f); le Conseil avait toutefois proposé de lever cette exclusion en autorisant une telle base de légitimation. Ce faisant, les opérations de big data auraient été facilitées (c'était d'ailleurs l'objectif poursuivi), mais au prix d'un affaiblissement substantiel du principe de finalité (24). De nombreuses critiques avaient ainsi été émises, notamment par le Groupe 29 (25). Il aurait en effet été possible de corriger l'incompatibilité en identifiant une nouvelle base de légitimation. On permettait donc de pallier la méconnaissance du principe de finalité par le respect d'une autre condition. Or, il s'agit de deux conditions distinctes et cumulatives. Le texte avait heureusement été revu pour limiter les hypothèses dans lesquelles les traitements ultérieurs pour des finalités incompatibles avec les finalités initiales sont permis.

On peut également échapper à l'interdiction d'un traitement ultérieur incompatible avec les finalités initiales si ce traitement est réalisé, entre autres, à des fins statistiques. Des garanties appropriées doivent toutefois être prévues. L'article 89, § 1er, du Règlement impose ainsi la mise en place de « mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données. Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. Chaque fois que ces finalités peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière ».

9. Principe de minimisation des données. Le principe de minimisation des données est consacré à l'article 5, § 1er, c), aux termes duquel les données à caractère personnel doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Cette exigence de proportionnalité figurait déjà dans la directive 95/46/CE et la LVP, qui exigeaient toutefois que les données soient « non excessives » (et pas « limitées à ce qui est nécessaire »).

Le considérant n° 39 précise que « les données à caractère personnel ne devraient être traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens ».

Dans le contexte du big data, le respect de ce principe pourrait poser de réelles difficultés.

Par nature, les opérations de big data supposent que de grands volumes de données soient examinés, sans savoir, *a priori*, si elles se révéleront pertinentes, adéquates ou même utiles dans le cadre du traitement. C'est d'ailleurs l'élément-clé du big data: utiliser le plus de données possibles, pour espérer en tirer une information utile

(24) À ce sujet, voy. C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, *o.c.*, pp. 18 et s.
(25) Groupe 29, « Opinion 03/2013 on purpose limitation », 2 avril 2013, WP 203, pp. 36-37.

dans le cadre des traitements envisagés par les compagnies d'assurances (en termes de *scoring* des clients ou à la suite d'un accident, par exemple).

Une analyse au cas par cas devra donc être effectuée par le responsable du traitement, pour s'assurer que la finalité poursuivie, à la supposer légitime et respectueuse des autres exigences applicables, ne peut pas être atteinte autrement, par des mesures plus respectueuses des droits de la personne concernée.

S'agissant par exemple des données collectées par un véhicule concernant la manière de conduire de la personne, et qui seraient justifiées par une optimisation des entretiens ultérieurs réalisés par le constructeur, on peut sérieusement douter que l'enregistrement des données de localisation du véhicule ou de certaines informations sur le mode de conduite soient nécessaires à la finalité projetée. En général, il sera en effet possible d'atteindre le résultat attendu sans procéder à un tel traitement, ne serait-ce que parce que de nombreux constructeurs ne collectent pas de telles données.

10. Principe d'exactitude. L'article 5, § 1er, d), du Règlement exige que les données soient « exactes et, si nécessaires, tenues à jour ». Cette disposition ajoute que « toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ».

Ce principe d'exactitude était déjà consacré par la directive 95/46/CE.

Des difficultés sont également à prévoir dans le contexte du big data, qui repose sur l'analyse d'une grande quantité de données, sans se soucier, *a priori*, de leur exactitude. Les sources de la collecte sont à ce point nombreuses et variées que, sans surprise, pour certaines d'entre elles, il est permis de douter de leur conformité à la réalité (on pense par exemple aux données collectées sur les réseaux sociaux).

11. Principe de limitation de la conservation. Ce principe est énoncé à l'article 5, § 1er, e), du Règlement, aux termes duquel les données doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement 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 1er, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée ».

Il semble que, pour la plupart, les données exploitées dans le cadre du big data ont été collectées assez récemment. À terme, la compagnie d'assurances responsable du traitement peut toutefois être intéressée à conserver celles-ci sur une longue période, de manière à en tirer autant d'informations utiles que possible, ce qui pourrait heurter ce principe de limitation de la conservation. Ces compagnies devront donc être attentives à cette exigence et mettre en place des mesures techniques et organisationnelles en interne, pour s'assurer que les données soient effacées le moment venu.

La fixation de ce moment se confondra généralement avec la période de prescription applicable ou avec des délais de conservation éventuellement imposés par des législations spécifiques ressortissant au droit des assurances. On sait toutefois qu'en matière d'archivage, cette question peut être source d'incertitude et de discussions. Par prudence, le choix d'une période de conservation relativement longue (correspondant au délai de prescription le plus long) est recommandé, ce qui sera utile dans l'hypothèse du big data.

12. Principe de responsabilité (accountability). Conformément au principe de responsabilité, tel qu'énoncé à l'article 5, § 2, du RGPD, il incombe au responsable du traitement de respecter les principes énoncés au paragraphe 1er, tout en étant en mesure d'en apporter la preuve. Aussi est-il recommandé de mettre en place des mesures organisationnelles, en interne, qui garantissent leur respect effectif, et de les documenter à suffisance. En cas de plainte ou de demande d'une autorité de contrôle compétente, la compagnie d'assurances pourra ainsi établir qu'elle agit en parfaite conformité avec la législation applicable.

En lien avec ce principe, le Règlement impose diverses obligations qui participent de cet objectif et visent à prévenir, autant que possible, les risques engendrés par les traitements de données. En remplacement de l'obligation de notification (ou de déclaration) préalable auprès des autorités de contrôle, dont l'effectivité pouvait être sérieusement questionnée, le Règlement prévoit désormais l'obligation de tenir un registre des activités de traitement (26) et de procéder, dans certains cas, à une analyse d'impact (27).

Sur ce dernier point, il est prévu que « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ». L'objectif est de s'assurer qu'en réponse à cette analyse d'impact, des mesures soient prises en vue de réduire le risque ainsi identifié et correctement circonscrit. Qu'en est-il dans le contexte du big data? Il est clairement visé par le considérant n° 91 du Règlement (28), qui mentionne l'hypothèse dans laquelle « des données à caractère personnel sont traitées en vue de prendre des décisions relatives à des personnes physiques spécifiques à la suite d'une évaluation systématique et approfondie d'aspects personnels propres à des personnes physiques sur la base du profilage desdites données ». On mentionne aussi l'hypothèse dans laquelle « l'autorité de contrôle compétente considère que le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées [...] parce qu'elles sont effectuées systématiquement à grande échelle ». Le cas échéant, les compagnies d'assurances devront par conséquent réaliser une telle analyse d'impact pour les traitements big data qu'elles envisagent.

(26) Art. 30 du RGPD.
(27) Art. 35 du RGPD.
(28) En ce sens, voy. C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, *o.c.*, p. 30. À ce sujet, voy. aussi Groupe 29, « Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk', for the purposes of Regulation 2016/679 », WP 248, 4 avril 2017.

III. Le big data à l'aune du principe de licéité

13. Licéité. Le RGPD fixe, *a priori*, des conditions ou bases de licéité de traitement en distinguant selon que les données traitées sont, soit « non sensibles », soit, au contraire, « sensibles » ou, selon le vocable utilisé par le Règlement, « particulières ».

Dans la présente contribution, nous nous limitons à celles qui sont les plus susceptibles d'être invoquées en matière de big data: le consentement, la base contractuelle et l'intérêt légitime du responsable du traitement.

A. Le consentement

14. Portée. Le consentement est l'une des bases de licéité fixée *a priori* par le législateur européen; consentement qui doit répondre, lui-même, à des conditions précisées à l'article 7 du RGPD.

Comme cela a déjà été exposé dans de précédentes contributions du présent *Dossier*, le RGPD a renforcé, dans une volonté de confirmer le principe d'autodétermination informationnelle de la personne concernée, la notion de consentement, par rapport à la directive 95/46/CE qui était assez imprécise sur ce point.

Un des aspects de ce renforcement est la nécessité d'un consentement pour l'ensemble des finalités envisagées par le responsable du traitement mais également de manière expresse.

En effet, le considérant 32 du RGPD précise que:

> « Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site Internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles. Si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé ».

On doit cependant analyser ce consentement de manière différenciée, selon que l'on se situe dans une collecte directe ou, au contraire, indirecte.

15. Collecte directe. Si la compagnie d'assurances entend utiliser des données collectées directement auprès de l'assuré lui-même, il faudra que cet assuré marque son consentement de manière univoque.

Si ce consentement est recueilli, par exemple, à travers le site Internet de la compagnie, cela devra se faire via une case à cocher et non pas via une case préalablement cochée par la compagnie. Dans la première hypothèse, il appartient au client de cocher lui-même la case (acte positif) tandis que, dans la seconde hypothèse, le client doit décocher la case, ce qui est proscrit par le RGPD.

Par ailleurs, il ne faudrait pas que la compagnie d'assurances abuse de sa position pour « extorquer » un consentement. Ainsi, le considérant 43 précise, entre autres, que « le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution ».

Il convient également d'avoir égard à la période durant laquelle le consentement a été donné au regard de l'entrée en vigueur du RGPD. En d'autres termes, si le consentement a été recueilli sous l'empire de la directive 95/46/CE, qui est moins précise quant aux conditions de validité à satisfaire, la compagnie d'assurances devra s'assurer, et à condition que le traitement soit fondé sur le consentement, que ce consentement répond aux conditions fixées par le RGPD. En effet, son considérant 171 précise que « lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable du traitement puisse poursuivre le traitement après la date d'application du présent règlement ».

Il est donc utile que les compagnies d'assurances procèdent à une analyse des consentements obtenus à ce jour pour, le cas échéant, se conformer au RGPD avant mai 2018.

16. Collecte indirecte. L'hypothèse visée, en l'espèce, est celle d'un traitement ultérieur utilisant des données provenant d'un tiers qui, lui, les a, la plupart du temps, collectées directement auprès de la personne concernée.

Ce cas de figure est visé par les articles 5, § 1er, b) et 6, § 4, du RGPD qui fixent les conditions dans lesquelles un traitement peut être considéré comme compatible avec le traitement initial. Nous ne traiterons pas des situations visées par l'article 5, § 1er, b), qui sont liées au traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. Même à considérer qu'il y a une finalité statistique, elle devrait rester assez limitée.

Pour rappel, l'article 6, §4 concerne « le traitement à une fin autre que celle pour laquelle les données ont été collectées qui n'est pas fondé sur le consentement de la personne concernée ». On peut prendre l'exemple de la compagnie d'assurances qui traite des données dans le cadre d'un service d'assurance impliquant une analyse de risque la plus précise que possible et en vue de pouvoir déterminer la prime qui devra être payée par l'assuré.

Si les données traitées sont collectées auprès d'un tiers et que la finalité du traitement n'était pas du tout liée à cette finalité nouvelle, il sera difficile de considérer qu'il y a compatibilité entre les deux finalités au moyen des critères mentionnés par cet article 6, §4, et qui ont déjà été exposés ci-dessus.

Notons qu'il n'existe pas d'équivalent à l'article 6, §4 pour les catégories particulières des données.

17. Catégories particulières de données. Les compagnies d'assurances sont en général intéressées par certaines catégories de données telles que les données relatives à la santé ou aux condamnations. Or, le RGPD octroie une protection accrue à ces données, qui sont considérées comme sensibles *in se*.

Un arrêt a été rendu par la Cour constitutionnelle dans le cadre d'une requête en annulation déposée contre la loi du 21 janvier 2010 modifiant la loi du 25 juin 1992 sur le contrat d'assurance terrestre en ce qui concerne les assurances du solde restant dû pour les personnes présentant un risque de santé accru. En vertu de cette loi, la Commission des assurances devait établir un code de bonne conduite à défaut de quoi le Roi était habilité à régler la question des questionnaires médicaux dans le cadre des assurances du solde restant dû pour les personnes présentant un risque de santé accru (29).

La Cour constitutionnelle a clairement rappelé que la proportionnalité devait être analysée au niveau des données afin d'éviter que des données non nécessaires à la finalité ne soient traitées et ainsi considéré que:

> « le législateur a pu estimer que l'utilisation de ces questionnaires devait être réglementée afin d'éviter que, dans le cadre de la conclusion d'un contrat d'assurance, des questions soient posées qui ne sont pas pertinentes ou qui sont excessives et qu'il soit ainsi porté atteinte de manière disproportionnée au droit au respect de la vie privée des intéressés. Il a également pu estimer que le fait que les assureurs exigent un examen médical complémentaire et demandent les résultats de celui-ci, en plus de l'utilisation d'un questionnaire médical, pouvait constituer une restriction disproportionnée du droit au respect de la vie privée de l'intéressé dans les cas où le montant assuré demeure limité » (30).

Pour sa part, la Cour européenne des droits de l'homme a également précisé que:

> « Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (préambule et article 5 de la Convention sur la protection des données et principe 7 de la recommandation R(87)15 du Comité des Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police) » (31).

(29) À noter que cette loi a entre-temps été remplacée par la loi du 4 avril 2014 relative aux assurances (voir art. 212 et s.).

(30) C.C., 10 novembre 2011, n° 166/2011, www.const-court.be, B.16.7.

(31) C.E.D.H., 4 décembre 2008 (S. et Marper c. Royaume-Unis), requêtes nos 30562/04 et 30566/04, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90052, al. 103.

La législation belge n'est pas en reste au niveau de la protection des informations médicales de l'assuré puisque l'article 61 de la loi du 4 avril 2014 relative aux assurances précise que:

> « Le médecin choisi par l'assuré peut remettre à l'assuré qui en fait la demande, les certificats médicaux nécessaires à la conclusion ou à l'exécution du contrat. Ces certificats se limitent à une description de l'état de santé actuel.
>
> Ces certificats ne peuvent être remis qu'au médecin-conseil de l'assureur. 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.
>
> 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 son état de santé futur.
> (...) »

On constate ainsi que la collecte de données médicales est particulièrement réglementée pour éviter que les assureurs n'exercent de pression sur les assurés pour obtenir des informations qui, certes leur seront bien utiles pour évaluer les risques, mais peuvent se révéler disproportionnées aux yeux du législateur.

Il est également utile de relever que la Cour européenne des droits de l'homme de Strasbourg a considéré que « les informations personnelles relatives à un patient appartiennent à sa vie privée » (32) et qu' « il est primordial d'avoir des règles claires et détaillées en matière de divulgation d'informations médicales confidentielles et qui offrent des garanties suffisantes contre le risque d'abus et d'arbitraire » (33). Cela fait dire à un auteur que « la Cour répète à cet égard que la protection des données à caractère personnel, en ce compris les informations médicales, est d'une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale » (34).

Par ailleurs, on doit rappeler que la Commission de la protection de la vie privée belge a eu l'occasion de préciser que « tout échange (ou toute catégorie d'échange) électronique pour lequel il est fait appel au consentement du patient (...), doit, au préalable, avoir été autorisé par le Comité sectoriel. Cela signifie que le Comité sectoriel vérifiera dans sa délibération que tout échange électronique satisfait aux conditions énumérées dans le formulaire de consentement et, de manière plus générale, aux principes de la vie privée » (35). Cela signifie, en d'autres mots, que le Comité sectoriel devra autoriser le transfert de données relatives à la santé entre le tiers vers la compagnie d'assurances, ce qui n'est pas automatique et loin s'en faut.

(32) J. HERVEG, « Décisions de la Cour européenne des droits de l'homme de Strasbourg », *Chronique de jurisprudence en droit des technologies de l'information et de la communication (2012-2014)*, *RDTI*, 2015, n^{os} 59-60, p. 94.

(33) *Ibid.*

(34) *Ibid.*

(35) Commission de la protection de la vie privée, délibération n° 12/047 du 19 juin 2012 relative au consentement éclairé d'une personne concernée concernant l'échange électronique de ses données à caractère personnel relatives à la santé et au mode d'enregistrement de ce consentement, p. 4, point 8, www.privacycommission.be/node/15649. Il est vrai que l'on ne connaît pas encore le sort réservé aux comités sectoriels après l'entrée en vigueur du RGPD.

De plus, le traitement de telles données relatives à la santé a pour finalité des prises de décision d'assurabilité ou non par rapport à l'assuré, ce qui n'est pas dénué de conséquences pour l'assuré au sens de l'article 6, § 4, d), du RGPD. Pour rappel, cet article impose au responsable de traitement, la compagnie d'assurances en l'espèce, de tenir compte, parmi d'autres éléments, « des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ». Or, les conséquences du traitement peuvent se révéler douloureuses pour l'assuré.

Il appert donc que le consentement de l'assuré s'avérera, la plupart du temps, indispensable dès lors que la compagnie d'assurances ne pourra bien souvent pas procéder à un traitement ultérieur et devra donc entamer un nouveau traitement *ab initio* pour les raisons qui viennent d'être évoquées ci-dessus.

B. Exécution d'un contrat

18. Données non sensibles. Une seconde condition de licéité, ayant une égale valeur à celle liée au consentement, est rencontrée si 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 » (36). Ainsi, un cadre contractuel peut donc rendre licite un traitement de données à caractère personnel.

Les contrats avec une compagnie d'assurances peuvent être visés par cette disposition. Elle pourrait donc servir de base à un traitement de données à caractère personnel.

Un certain nombre de conditions doivent cependant être respectées par la compagnie d'assurances pour rencontrer les exigences du RGPD.

- Il est d'abord requis que l'assuré soit partie au contrat et ait demandé que des mesures précontractuelles nécessitant un traitement de données soient prises. *A contrario*, la compagnie d'assurances ne pourra traiter des données à caractère personnel concernant une personne qui n'est pas partie au contrat ou qui n'a pas demandé de mesures précontractuelles. La compagnie d'assurances devra trouver une autre base de licéité pour effectuer le traitement.
- En outre, le traitement de données doit être nécessaire à l'exécution du contrat en question ou de mesures précontractuelles. Ainsi, la mise en place de cookies dans l'ordinateur de l'assuré ne pourra être considéré comme nécessaire à l'exécution du contrat liant la compagnie d'assurances à l'assuré. Même si cette opération peut ne pas être illégale en soi, elle devra trouver une autre base de licéité pour effectuer le traitement.

En l'espèce et dans l'hypothèse où on pourrait considérer que le traitement des données à caractère personnel de l'assuré entre dans le cadre de l'exécution d'un contrat ou de mesures précontractuelles, il n'en demeure pas moins que ce traitement doit être nécessaire.

(36) Art. 6, § 1er, b), du RGPD.

19. Catégories particulières de données. Si la base contractuelle constitue un fondement assez large en termes de traitement de données à caractère personnel non sensibles, il en va autrement lorsque la compagnie d'assurances traitera, par exemple, des données à caractère personnel relatives à la santé.

En effet, une telle base ne pourra être utilisée qu'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 sécurité sociale ou de protection sociale.

Or, il ne peut être considéré que les compagnies d'assurances entrent dans l'une de ces catégories, de sorte que de telles données ne pourront être traitées sur cette base de licéité.

Comme nous l'avons vu ci-dessus, les voitures et les accessoires qui l'équipent – qu'ils soient placés par le constructeur ou par l'usager lui-même – peuvent se révéler très loquaces en matière de comportement de conduite de l'assuré. Les informations ainsi délivrées seront très utiles lors d'un accident par exemple.

Cependant, les données collectées peuvent être en lien avec des infractions avérées ou potentielles. Or, l'article 10 du RGPD précise que « le traitement des données à caractère personnel relatives (...) aux infractions (...), ne peut être effectué que sous le contrôle de l'autorité publique ». S'il est regrettable que le Règlement ne soit pas plus précis sur ce qu'il entend exactement par « traitement de données à caractère personnel relatives aux infractions », les compagnies d'assurances devront à tout le moins se montrer prudentes lors de l'utilisation de données d'analyse du comportement de conduite routière de leurs assurés et veiller à ne pas traiter des données relatives aux infractions.

C. Intérêts légitimes du responsable du traitement

20. Notion. L'article 6, § 1er, f), du RGPD permet à la compagnie d'assurances de traiter des données à caractère personnel de son assuré si ce traitement est nécessaire aux fins de ses intérêts légitimes ou à celles d'un tiers, « *à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de [l'assuré] qui exigent une protection des données à caractère personnel, notamment lorsque [l'assuré] est un enfant* » (37). Il est utile de rappeler que l'assuré pourra faire valoir son droit d'opposition (38).

Cette base de licéité ne vaut cependant que pour les données non sensibles et non pour les données particulières telles que celles relatives à la santé ou à des infractions. Cela limite donc de façon importante les possibilités d'utilisation de cette base par une compagnie d'assurances.

De plus et dans l'hypothèse où la compagnie l'utilise, elle ne sera pas à l'abri d'un contrôle du juge à la demande de l'assuré qui pourrait considérer que « les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel » (39) prévalent sur ses intérêts légitimes.

(37) Art. 6, § 1er, f), du RGPD.
(38) CEPD, avis n° 7/2015, 19 novembre 2015, p. 11.
(39) Art. 6, § 1er, f), du RGPD.

IV. Les droits de l'assuré ou du preneur, personne concernée

A. Information

21. Principe. Une des pierres angulaires du RGPD est l'exigence de transparence de tout traitement à l'égard de la personne concernée. Cette transparence est, évidemment, tempérée par le devoir de confidentialité à l'égard des tiers.

Ce principe se retrouve à divers niveaux du Règlement, à commencer par l'obligation d'informer la personne concernée, telle qu'elle figure au chapitre III, section 2. Des différences sont prévues selon que les données sont collectées auprès de la personne concernée ou pas.

Pour certaines données, telles que celles relatives à la santé ou aux infractions, des informations complémentaires devraient être données comme cela est prévu au chapitre III de l'arrêté royal du 13 février 2001 portant exécution 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. Notons cependant que nous ne connaissons pas, au moment de la rédaction de la présente contribution, le sort qui sera donné à cet arrêté royal après l'entrée en vigueur du RGPD.

Il est utile de relever que le Contrôleur européen en protection des données a, dans un avis du 19 novembre 2015, consacré tout un chapitre à la transparence du traitement en l'intitulant « transparence: mettre un terme au profilage clandestin » (40). Cela démontre toute l'importance de l'information qui doit permettre, entre autres choses, à la personne concernée de « connaître la logique qui sous-tend le processus décisionnel » (41) et « d'aider les particuliers à mieux vérifier l'exactitude et l'équité des conclusions tirées par les organisations qui traitent les données et affectent les individus » (42). Il ajoute que ces mêmes particuliers « pourront mieux comprendre et peut-être rectifier les critères sous-jacents et les facteurs qui influencent la décision » (43).

22. Collecte auprès de l'assuré. La compagnie d'assurances sera obligée de délivrer un certain nombre d'informations à son assuré au moment de la collecte des données; informations qui sont précisées à l'article 13 du RGPD.

Il est intéressant de relever, en écho à ce qui a été exposé en termes de traitement ultérieur que « lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité » (44).

Cela implique donc que l'information est une contrainte, quel que soit le type de traitement (principal ou ultérieur).

(40) CEPD, avis n° 7/2015, 19 novembre 2015, p. 11.
(41) CEPD, avis n° 7/2015, 19 novembre 2015, p. 11.
(42) *Ibid.*
(43) *Ibid.*
(44) Art. 13, § 3, du RGPD.

23. Collecte auprès d'un tiers (45). Le RGPD impose à la compagnie d'assurances de fournir l'information à l'assuré dans un délai raisonnable après l'obtention des données à caractère personnel, sans que cela ne dépasse un mois en tenant compte des circonstances particulières dans lesquelles les données à caractère personnel sont traitées.

Si ces données à caractère personnel doivent être utilisées aux fins de communication avec l'assuré, l'information doit intervenir au plus tard au moment de la première communication à ce dernier.

Et si la compagnie d'assurances envisage, à son tour, de communiquer les données à un autre destinataire, l'information devra être délivrée au plus tard lorsqu'elles sont communiquées pour la première fois.

B. Droit d'accès, de rectification, d'opposition et de suppression

24. Droit d'accès (46). Le principe de transparence mentionné ci-dessus donne naissance à divers droits au profit de l'assuré, parmi lesquels figure le droit d'accès.

Ce droit d'accès est fondamental pour l'assuré afin qu'il puisse procéder à diverses vérifications, et notamment en vue de savoir si des données à caractère personnel le concernant sont traitées. Si la réponse est positive, il pourra alors, entre autres, prendre connaissance des données traitées et s'assurer que le traitement est conforme au RGPD et à la finalité annoncée.

Il a également le droit, lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, à toute information disponible quant à leur source.

De ce premier droit qui est, en quelque sorte, une porte d'entrée au contrôle du traitement pour la personne concernée, découle l'exercice d'autres droits tels que les droits de rectification, d'opposition, etc. (47)

25. Droit de rectification (48). L'assuré pourra demander la rectification de ses données à caractère personnel traitées par la compagnie d'assurances et qui sont inexactes.

Nous retrouvons ici un pendant à l'obligation d'exactitude exposée précédemment. En effet, la compagnie d'assurances se verra contrainte de modifier toutes les données inexactes mais aussi, le cas échéant, de revoir des décisions prises sur la base de données inexactes issues du big data.

26. Droit d'effacement ou droit à l'oubli (49). L'assuré pourra demander l'effacement de données le concernant dans un certain nombre de cas, et notamment l'absence de nécessité au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière; le retrait de son consentement ou l'absence de licéité.

(45) Art. 14 du RGPD.
(46) Art. 15 du RGPD.
(47) Voir C.J.C.E., 7 mai 2009 (Rijkeboer c. Pays-Bas), C-553/07.
(48) Art. 16 du RGPD.
(49) Art. 17 du RGPD.

À titre d'exemple, on peut imaginer que la compagnie d'assurances traite des données relatives à la santé dans le cadre de l'exécution du contrat et ce, sans le consentement de l'assuré. Ce dernier pourra demander l'effacement des données dès lors que le traitement n'est pas fondé sur une des bases de licéité analysées ci-dessus. En effet et comme nous l'avons déjà vu, la condition de licéité relative à l'exécution de contrat ne peut pas s'appliquer aux assurances dans le cadre desquelles des données particulières telles que des données relatives à la santé sont traitées.

De plus, la compagnie d'assurances ne pourra normalement pas faire valoir l'une des exceptions prévues à l'article 17, § 3, du RGPD pour s'opposer à la demande d'effacement (50).

27. Droit à la limitation du traitement (51). En vertu de ce nouveau droit prévu par le RGPD, l'assuré a le droit d'obtenir de la compagnie d'assurances la limitation du traitement dans certains cas, tels qu'une contestation relative à l'exactitude des données à caractère personnel, et ce, durant une durée suffisante pour permettre à la compagnie de procéder aux vérifications nécessaires, au caractère licite du traitement mais sans utilisation de son droit à l'effacement par l'assuré.

La compagnie d'assurances pourrait également être amenée, alors même qu'elle n'aurait plus besoin des données à caractère personnel de l'assuré, à devoir les conserver tout en en limitant le traitement, au motif qu'elles sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice. Cette situation peut bien évidemment intervenir en matière d'assurance dès lors que le contrat pourrait être résilié alors même que l'assuré serait susceptible de devoir accéder aux données traitées par la compagnie afin de pouvoir se défendre en justice à l'égard d'un tiers mettant sa responsabilité en cause, par exemple, ou même pour faire valoir ses droits à l'égard de la compagnie d'assurances elle-même. Ce droit à la limitation du traitement permet à l'assuré de voir ses données conservées alors que la compagnie d'assurances devrait les effacer en vertu du même Règlement.

À noter que si la limitation du traitement est levée pour une raison ou une autre, la compagnie d'assurances devra en informer l'assuré avant que cette limitation ne soit levée (52).

(50) L'article 17, § 3, du RGPD prescrit que le responsable du traitement peut s'opposer à une demande d'effacement « dans la mesure où [le] traitement est nécessaire:
a) à l'exercice du droit à la liberté d'expression et d'information;
b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3;
d) 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 1er, dans la mesure où le droit visé au paragraphe 1er est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou
e) à la constatation, à l'exercice ou à la défense de droits en justice ».
(51) Art. 18 du RGPD.
(52) Art. 18, § 3, du RGPD.

On relève encore que, dans l'hypothèse où la compagnie d'assurances a communiqué les données concernant l'assuré à un tiers, elle doit notifier à ce tiers toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement. Elle devra, en outre, fournir à l'assuré des informations sur ces destinataires en cas de demande de sa part (53).

28. Droit d'opposition (54). L'assuré a, enfin, le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel le concernant fondé sur, entre autres, les intérêts légitimes de la compagnie d'assurances (55), en ce compris un profilage fondé sur cette même base de licéité.

La compagnie d'assurances pourra cependant s'opposer à la demande de l'assuré si elle démontre « qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de [l'assuré], ou pour la constatation, l'exercice ou la défense de droits en justice » (56).

C. Profilage

29. Données normales (57). La compagnie d'assurances est souvent tentée de procéder à l'établissement du profil de ses assurés afin de pouvoir évaluer le risque et pouvoir adapter son attitude à l'égard de ces derniers. C'est du reste dans ce but précis qu'elle voudra généralement utiliser le big data.

Ce profilage est autorisé s'il est, par exemple, nécessaire à la conclusion ou à l'exécution d'un contrat d'assurance ou si la compagnie a obtenu le consentement de l'assuré. En contrepartie, elle devra mettre en « œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes [de l'assuré], au moins du droit de la personne concernée d'obtenir une intervention humaine de [sa] part, d'exprimer son point de vue et de contester la décision » (58) qui serait prise sur la base de ce profilage.

30. Données particulières (59). Le profilage par une compagnie d'assurances, ou à tout le moins les décisions qui en découleront, ne pourra s'effectuer sur les données sensibles telles que celles relatives à la santé ou aux infractions, à moins qu'il y ait eu consentement de l'assuré (60).

Dans cette hypothèse, la compagnie d'assurances devra mettre en place « des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes » (61) de l'assuré. Encore faut-il que le consentement réponde aux conditions de validité analysées ci-dessus.

(53) Art. 19 du RGPD.
(54) Art. 21 du RGPD.
(55) Art. 6, § 1er, f), du RGPD.
(56) Art. 21, § 1er, *in fine* du RGPD.
(57) Art. 22, §§ 2 et 3, du RGPD.
(58) Art. 22, § 3, du RGDP.
(59) Art. 22, § 4, du RGPD.
(60) Les autres exceptions ne peuvent, à notre estime, s'appliquer dans le cadre des assurances.
(61) Art. 22, § 4, du RGDP.

Cette exigence de consentement limite de manière importante les possibilités de profilage et la compagnie d'assurances devra veiller à ne pas exercer de pression, de quelque nature que ce soit, sur l'assuré afin d'obtenir son consentement au risque de voir le consentement invalidé mais aussi de subir des sanctions pécuniaires pouvant aller jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédant la décision, ou s'élever jusqu'à 20 millions d'euros, le montant le plus élevé étant retenu (62).

V. Conclusion

31. Le big data entre risques et enjeux. Si le big data est attirant pour les compagnies d'assurances dans leur quête d'une appréciation du risque (entre autres utilisations possibles du big data), le traitement des données collectées peut s'avérer très hasardeux si pas impossible, en tout cas pour les données les plus intéressantes.

Comme nous l'avons vu, le RGPD a renforcé certains principes par rapport à la directive 95/46 de sorte qu'il faudra que les compagnies d'assurances adaptent leur comportement si tel n'est pas déjà le cas.

Si l'on peut aisément comprendre que l'évaluation du risque constitue un enjeu économique important, cela ne peut se faire au détriment de la protection des données à caractère personnel des assurés qui ont droit à leurs propres secrets sans pour autant, bien entendu, cacher des éléments que la loi et la jurisprudence les obligent à révéler. S'ils abusent de ce droit à la protection de leurs données en procédant à une déclaration du risque inexacte, de manière volontaire ou pas, ils pourront en être sanctionnés.

Les compagnies d'assurances risquent également, dans l'utilisation du big data, d'être vite confrontées à un problème de justification sur le plan de la proportionnalité du traitement et de son caractère nécessaire au regard du principe de minimisation mis en place par le Règlement. Il conviendra donc à ces compagnies de se poser les bonnes questions afin d'éviter de se trouver face à la justice qui ne manquera pas de les frapper de lourdes sanctions qui, pour rappel, peuvent aller jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédant la décision ou atteindre un montant de 20 millions d'euros. Le respect des données à caractère personnel des assurés est à ce prix.

Le Règlement donne, par ailleurs, une place importante à l'information qui permettra réellement à l'assuré, d'une part, de savoir si des données sont traitées par la compagnie d'assurances et lesquelles et, d'autre part, de pouvoir exercer ses droits en toute connaissance de cause.

Le consentement renforcé par le nouveau texte donne une arme complémentaire à l'assuré contre les abus qui peuvent être commis par les compagnies d'assurances mais le responsabilise également. En effet, le consentement donné par l'assuré, à condition qu'il soit valide au sens du Règlement, ouvrira de nombreuses possibilités de traitement au profit de la compagnie d'assurances, et ce, en toute légalité. Cependant et afin de contrebalancer les conséquences de ce consentement, l'assuré pourra utiliser ses droits pour contrôler l'usage que la compagnie d'assurances en fera et

(62) Art. 83, § 5, du RGPD.

ainsi s'assurer que le traitement réellement effectué est conforme à celui annoncé et sur lequel porte le consentement.

En matière d'assurances, le big data a donc cette particularité de réunir, dans un même concept, des capacités énormes d'évaluation des risques mais aussi un risque tout aussi énorme d'atteinte à la protection de la personne. Antoinette ROUVROY n'a-t-elle pas déclaré que « l'enjeu, ce n'est pas la donnée personnelle, mais bien plutôt la disparition de la 'personne' dans les deux sens du terme. Il nous devient impossible de n'être 'personne', d'être 'absents' (nous ne pouvons pas ne pas laisser de traces) et il nous est impossible de compter en tant que 'personne'. Ce que nous pourrions dire de nous-mêmes ne devient-il pas redondant, sinon suspect, face à l'efficacité et à l'objectivité machinique des profilages automatiques dont nous faisons l'objet? » (63)

(63) A. ROUVROY, « Big data: l'enjeu est moins la donnée personnelle que la disparition de la personne », *Le Monde*, 22 janvier 2016, http://binaire.blog.lemonde.fr/2016/01/22/le-sujet-de-droit-au-peril-de-la-gouvernementalite-algorithmique/.