L'ARTICULATION DU RGPD AVEC L'EU DIGITAL PACKAGE (DSA, DORA, DA ET AIA) – PREMIERS ENSEIGNEMENTS DANS LE SECTEUR DES ASSURANCES

Chloé ANTOINE (1)

&

Hervé JACQUEMIN (2)

(1) Chercheuse au CRIDS/NADI (UNamur) et avocate au barreau de Namur (Lexing).
(2) Professeur à l'UNamur, directeur du CRIDS/NADI, avocat au barreau de Bruxelles (Lime).

INHOUDSTAFEL / TABLE DES MATIÈRES

SAMENVATTING

Op het niveau van de Europese Unie wordt het digitaal recht gekenmerkt door de aanneming van alsmaar meer teksten die een omkadering moeten bieden voor zaken die zo divers zijn als artificiële intelligentie, cyberbeveiliging en gegevensdeling. In tal van situaties zullen deze teksten simultaan met de Algemene Verordening Gegevensbescherming (AVG) van toepassing zijn, gezien de centrale plaats die persoonsgegevens in de digitale omgeving innemen. De samenhang van de bepalingen in deze teksten en de bepalingen van de AVG zou in sommige gevallen voor problemen kunnen zorgen – ook op het gebied van verzekeringen, waar persoonsgegevens haast systematisch worden verwerkt.

Deze bijdrage onderzoekt een aantal van deze teksten – de Digital Services Act (DSA), de Digital Operational Resilience Act (DORA), de Data Act (DA) en de AI Act (AIA) – om te belichten voor welke uitdagingen ze ons plaatsen wanneer ze simultaan met de AVG worden toegepast, in het bijzonder in de context van verzekeringen.

De DSA omkadert de activiteit van tussenhandeldiensten en platformen. Op het gebied van verzekeringen zouden de moeilijkheden qua samenhang beperkt moeten blijven. De maatregelen die de DSA voorschrijft, zouden immers een aanvulling moeten blijken te vormen op die van de AVG, met name wanneer het over onlinereclame of profilering gaat.

DORA, dat de operationele veerkracht van de financiële entiteiten (inclusief de verzekeringsondernemingen en -tussenpersonen) moet garanderen, convergeert op meer punten met de AVG: zo vindt men in DORA soortgelijke vereisten als in de AVG (waarborgen inzake veerkracht, beschikbaarheid en geheimhouding, een procedure in geval van een inbreuk in verband met gegevens of een ICT-gerelateerd incident, de strikte omkadering van de inhoud van contracten enz.).

De DA heeft dan weer vooral tot doel gegevensdeling op het gebied van het Internet of things mogelijk te maken en te omkaderen. De verplichtingen die deze verordening hieromtrent oplegt, zou men kunnen opvatten in de zin dat zij aan gebruikers van verbonden producten of aanverwante diensten een “recht op inzage” en een “recht op gegevensoverdraagbaarheid” met een specifieke reikwijdte toekennen. Op het vlak van verzekeringen zouden de DA en de AVG meestal simultaan moeten worden toegepast. We voorzien geen grote moeilijkheden qua samenhang tussen deze twee instrumenten, in de eerste plaats wegens de complementariteit van de rechten op inzage en gegevensoverdraagbaarheid waarin de DA en de AVG voorzien wanneer de gebruiker een ‘betrokkene’ is, in de tweede plaats wegens de in de DA opgenomen hiërarchiebepalende clausule die stelt dat de AVG-bepalingen bij een conflict voorrang krijgen.

De AVG en de AI Act, ten slotte, zouden wat verzekeringen betreft, regelmatig simultaan moeten worden toegepast: AI-systemen moeten immers worden getraind met gegevens (en dat kunnen persoonsgegevens zijn) en het doeleinde ervan is zeer vaak content genereren of oplossingen vinden in verband met geïdentificeerde of identificeerbare natuurlijke personen, met name in het kader van geautomatiseerde beslissingen. Hierbij zal de uitdaging erin bestaan het gebruikte AI-systeem en de betrokken partijen op correcte wijze te kwalificeren. Moeilijkheden zijn daarbij niet uitgesloten voor AI-systemen met een hoog risico, met name als we artikel 22 van de AVG en de hiermee overeenstemmende verplichtingen van de AI Act samennemen.

RÉSUMÉ

Au niveau de l'Union européenne, le droit du numérique est marqué par l'adoption sans cesse croissante de textes visant à encadrer des thématiques diverses telles que l'intelligence artificielle, la cybersécurité ou le partage de données. Dans de nombreuses situations, ces textes s'appliqueront en même temps que le règlement général sur la protection des données (RGPD) en raison de la place centrale qu'occupent les données à caractère personnel dans l'environnement numérique. L'articulation des dispositions contenues dans ces textes et des dispositions du RGPD pourrait, dans certains cas, poser des difficultés, y compris dans le domaine des assurances où les traitements de données à caractère personnel sont presque systématiques.

La présente contribution examine certains de ces textes – le Digital Services Act (DSA), le Digital Operational Resilience Act (DORA), le Data Act (DA) et l'AI Act (AIA) – dans une optique de mise en lumière des enjeux qu'ils posent en cas d'application simultanée avec le RGPD, en particulier dans le domaine des assurances.

Le DSA encadre l'activité des services intermédiaires et des plateformes. En matière d'assurances, les difficultés d'articulation devraient rester limitées. Les mesures prescrites par le DSA devraient en effet se révéler complémentaires à celles du RGPD, notamment en matière de publicité en ligne ou de profilage.

S'agissant de DORA, dont l'objet est de garantir la résilience opérationnelle des entités financières (y compris, dès lors, les compagnies d'assurances et les intermédiaires), les points de convergence sont plus nombreux : dans DORA, on trouve ainsi des exigences similaires à celles du RGPD (garanties de résilience, disponibilité et confidentialité, procédure en cas de violation des données ou d'incident lié aux TICs, contenus des contrats strictement encadrés, etc.).

Le DA a quant à lui notamment pour objectif de permettre et d'encadrer le partage de données dans le domaine de l'Internet des objets. Les obligations qu'il impose en la matière pourraient être perçues comme accordant aux utilisateurs de produits connectés et de services connexes un « droit d'accès » et un « droit à la portabilité des données » de portée spécifique. Dans le domaine des assurances, l'application du DA et du RGPD devrait, la plupart du temps, être simultanée. L'on ne présage pas de grandes difficultés d'articulation entre ces deux instruments en raison, d'une part, de la complémentarité des droits d'accès et à la portabilité des données prévus par le DA et le RGPD lorsque l'utilisateur est une « personne concernée » d'autre part, de la clause de hiérarchie, contenue dans le DA, faisant prévaloir les dispositions du RGPD en cas de conflit.

Enfin, le RGPD et l'AI Act devraient régulièrement être appliqués de manière simultanée en matière d'assurances : les systèmes d'IA doivent en effet être entraînés sur des données (qui peuvent être à caractère personnel) et leur finalité est très souvent de produire du contenu ou de dégager des solutions en lien avec des personnes physiques identifiées ou identifiables, notamment dans le cadre de décisions automatisées. L'enjeu sera notamment de qualifier correctement le système d'IA utilisé, ainsi que les parties impliquées. Des difficultés ne sont pas exclues, pour les systèmes d'IA à haut risque, notamment, au moment d'articuler l'article 22 du RGPD et les obligations correspondantes de l'AI Act.

1. Florilège de nouveaux textes en droit européen du numérique. En droit de l'Union, la législature 2019-2024 a été marquée par de nombreuses propositions de la Commission visant à réformer, généralement en profondeur, le droit du numérique au sens large. Les textes sont mieux connus par l'acronyme qui les désigne : DA, DGA, DSA, DMA, FIDA, AIA, DORA, NIS2, eIDAS2, DSP3, MiCA, etc.

Diverses thématiques sont concernées : des données à l'intelligence artificielle, en passant notamment par les services de paiement, les services intermédiaires en ligne ou la cybersécurité. L'objectif des nouvelles règles est d'assurer un niveau élevé de protection au bénéfice des citoyens, des consommateurs et des entreprises, dans un environnement où le numérique occupe une place sans cesse croissante, et présente autant d'opportunités que de risques pour tous les acteurs concernés.

Au terme d'un parcours législatif parfois animé, au cours duquel les textes initiaux ont pu faire l'objet de modifications majeures, plusieurs directives et règlements ont finalement été adoptés et sont entrés en application (ou le seront dans les mois à venir). Sans prétendre à l'exhaustivité (3), nous avons choisi d'analyser certains de ces textes, pour illustrer la diversité des enjeux qu'ils posent en droit des assurances, lorsqu'ils doivent être appliqués en même temps que le règlement général sur la protection des données (4) (ou RGPD).

2. Articulation de ces textes avec les règles en matière de protection des données dans le secteur des assurances. Le RGPD, adopté en 2016, est l'un des textes phares de la précédente législature : il vise en effet à garantir le droit fondamental des personnes physiques à la vie privée et à la protection de leurs données à caractère personnel (5), en leur octroyant des droits subjectifs (droit d'accès, de rectification, de portabilité, etc.) et en imposant diverses exigences aux responsables du traitement et à leurs sous-traitants éventuels (sécurité, registre, analyse d'impact, etc.). Pour s'y conformer, les entreprises ont été amenées à revoir certaines pratiques, parfois de manière radicale.

Dans l'environnement numérique au sens large, avec le recours aux applications mobiles, aux e-mails ou aux sites internet, ainsi qu'à la multitude de services et de contenus qu'ils permettent d'offrir et d'échanger, les données – qu'elles soient, ou pas, à caractère personnel – sont omniprésentes. Elles constituent le moyen et, dans un grand nombre de cas, la fin de certaines activités menées en ligne (eu égard à leur valeur économique).

Logiquement, il conviendra donc d'articuler les dispositions du RGPD et celles de ces nouveaux textes, dès lors qu'elles devraient s'appliquer de manière concurrente (et donc, en même temps) dans de nombreuses hypothèses, leurs champs d'application respectifs étant par ailleurs relativement larges. Le constat pourra se vérifier dans plusieurs secteurs, et notamment en matière d'assurance.

---

(3) Pour un panorama de ces textes, voy. H. JACQUEMIN et A. MICHEL (dir.), *Chronique de législation en droit européen du numérique 2020-2023 (1ère partie), R.D.T.I*, 2023/92-93, 266 p.

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

(5) Celui-ci est par ailleurs consacré à l'article 8 de la Charte des droits fondamentaux de l'Union européenne, et dans divers autres textes internationaux et nationaux.

3. Plan et limites de la présente contribution. La présente contribution a pour objet de présenter certains textes tirés de l'EU Digital Package, en mettant en évidence les enjeux qu'ils posent lorsqu'ils sont appliqués en même temps que le RGPD, dans le domaine des assurances. Il ne s'agit donc pas d'analyser de manière systématique et exhaustive toutes les nouvelles directives et tous les nouveaux règlements, souvent longs et complexes, mais uniquement de les présenter avec la double limite (i) d'une application concurrente avec le RGPD, (ii) dans le domaine des assurances (6).

Plus précisément, après un exposé général sur les difficultés résultant de l'application simultanée de plusieurs textes normatifs (*infra*, point I), on présente une vue panoramique et générale de l'articulation du RGPD avec deux règlements (UE) spécifiques, pour illustrer leur complémentarité (*infra*, partie II) : le règlement sur les services numériques (7) (ou DSA, pour *Digital Services Act*) et le règlement sur la résilience opérationnelle numérique du secteur financier (8) (ou DORA, pour *Digital Operational Resilience Act*).

Ensuite, nous analysons plus en détails les enjeux posés par la possible application simultanée – et sans doute plus délicate – du RGPD et de deux textes particulièrement importants en droit des assurances (*infra,* partie III) : le règlement sur les données (9) (ou DA, pour *Data Act*) et le règlement sur l'intelligence artificielle (10) (ou *AIA,* pour *AI Act*). Par souci de clarté, nous prendrons notamment comme fil rouge permettant d'illustrer l'application de ces textes en droit des assurances l'hypothèse des voitures connectées et des assurances « *Pay How You Drive* » (ou « *Pay As You Drive* »).

1. Dans quels cas l'articulation entre les textes pourrait-elle engendrer des difficultés ?

4. Champs d'application convergents. Pour que la question de l'articulation éventuelle des textes se pose, encore faut-il que leurs champs d'application matériel,

(6) Pour un commentaire de l'impact du RGPD dans le secteur des assurances, voy. D. De Bot, « De gevolgen van de Algemene Verordening Gegevensbescherming voor de verzekeringssector – Enkele kritische bedenkingen », *Bull. Ass.*, 2016, pp. 127 et s. ; J.-F. Henrotte et F. Coton, « L'impact du R.G.P.D. dans le secteur des assurances : comment s'y conformer ? », *For. ass.*, 2018/185, pp. 107-111 ; J.-M. Binon, « Assurances de personnes et protection des données personnelles : un mariage tumultueux à l'ombre du RGPD », *R.D.C.*, 2021, pp. 1949 et s. ; L.-A. Nyssens, « La conformité des entreprises d'assurance au RGPD », *Bull. Ass.*, 2023/2, pp. 148 et s.

(7) Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), *J.O.*, L 277 du 27 octobre 2022.

(8) Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) n° 2016/1011, *J.O.*, L 333 du 27 décembre 2022.

(9) Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données), *J.O.*, L du 22 décembre 2023.

(10) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), *J.O.*, L du 12 juillet 2024.

personnel et spatial soient convergents, autrement dit que l'hypothèse visée – un traitement de données automatisé sans intervention humaine dans le cadre de la conclusion d'un contrat d'assurance à travers une application mobile, par exemple – soit soumise aux règles prévues par les différentes dispositions envisagées (le DSA et le RGPD, par exemple).

Une analyse au cas par cas doit donc être menée.

S'agissant du RGPD, on rappelle qu'il s'applique aux traitements de données à caractère personnel d'une personne physique (11). Aucune limitation n'est donc posée en lien avec la matière concernée ou le secteur d'activités. Sauf exception, les traitements de données à caractère personnel par les compagnies d'assurances et les intermédiaires d'assurances sont par conséquent soumis au RGPD.

Sur le plan personnel, les principales obligations reposent sur le responsable du traitement (ou les responsables conjoints) et, le cas échéant, sur le sous-traitant, en vue de protéger les droits des personnes concernées (12).

Le champ d'application territorial est quant à lui défini à l'article 3 et il est particulièrement large puisqu'il vise également les traitements de données des personnes concernées se trouvant sur le territoire de l'Union par des responsables du traitement ou des sous-traitants établis dans un pays tiers.

Nous mettrons ces concepts en perspective en examinant, par la suite, le domaine d'application des textes retenus pour la présente contribution.

5. Règles matérielles et sanctions en cas de non-respect. Dans l'hypothèse où un même cas d'espèce est soumis au RGPD et à un autre texte de droit de l'Union, aucune difficulté ne se posera si les règles matérielles prévues par chacun d'eux sont différentes et complémentaires (des obligations d'information portant sur des éléments distincts, par exemple).

Des difficultés pourraient, par contre, survenir si l'application simultanée des règles applicables conduit à des situations incohérentes, voire à des contradictions (la pratique est autorisée par le texte A et interdite par le texte B). Des solutions devront également être dégagées si les autorités chargées de mettre en œuvre les textes, notamment en recherchant et en sanctionnant les infractions sont différentes et/ou lorsque les sanctions susceptibles d'être prononcées ne sont pas les mêmes.

A l'évidence, il est inutile de présenter ici toutes les règles matérielles prévues par le RGPD. On se limite à rappeler qu'il pose divers principes, notamment en termes de licéité du traitement, de transparence ou de minimisation des données. La per-

(11) Art. 2, § 1er, du RGPD. Les notions de « données à caractère personnel » et de « traitement » sont définies à l'article 4 du règlement (points 1 et 2). Voy. C. DE TERWANGNE, « Définitions clés et champ d'application du RGPD », *Le règlement général sur la protection des données (RGPD/GDPR) – Analyse approfondie*, Bruxelles, Larcier, 2018, pp. 67 et s. ; K. JANSSENS et M. NUYTTEN, « De Algemene Verordening Persoonsgegevens : van theorie naar praktijk – Le Règlement général sur la Protection des Données : de la théorie à la pratique », *R.D.C.*, 2018, pp. 401 et s. ; J. DOORNAERT, *Le RGPD et sa mise en œuvre en droit belge*, Diegem, Kluwer, 2019, pp. 27 et s.

(12) Les notions de « responsable du traitement » et de « sous-traitant » sont définies à l'article 4 du règlement (points 7 et 8).

sonne concernée se voit également reconnaître un certain nombre de droits, en termes d'accès, de portabilité, de rectification, de prise de décision individuelle automatisée ou de profilage. Les responsables du traitement (et/ou les sous-traitants) doivent ainsi respecter des obligations corrélatives, tout en garantissant la sécurité des données à caractère personnel, dans le respect du principe de responsabilité. A défaut, des sanctions peuvent être prononcées par les autorités compétentes (en Belgique, l'Autorité de protection des données).

6. Principes permettant d'articuler les règles dont les conditions d'application sont convergentes, en établissant une priorité entre elles. Lorsque plusieurs textes sont potentiellement applicables à un même cas d'espèce, avec des risques d'incohérences ou de contradictions, il importe, dans un premier temps, d'analyser les textes en conflit potentiel pour déterminer s'ils contiennent une disposition visant à les articuler avec une autre réglementation.

A défaut, il convient de se pencher sur les principes généraux en la matière, exprimés notamment par les adages *specialia generalibus derogant* et *lex posterior priori derogat*.

Conformément à l'adage *specialia generalibus derogant,* « la norme qui règle spécialement une question prime celle qui énonce une disposition générale » (13). Son application exige d'identifier la question régie par les normes concurrentes et de comparer celles-ci pour distinguer le genre et l'espèce (14). En pratique, l'exercice n'est pas forcément simple : on peut en effet arriver à la conclusion que les textes constituent deux normes spéciales, réglant, chacun en ce qui le concerne, un aspect de la question, sous l'angle de protection des données pour le RGPD et de la sécurité du produit que constitue l'IA, en termes de risques, pour l'AI Act.

L'adage *lex posterior priori derogat* pourrait également être invoqué. Il signifie que « la norme chronologiquement postérieure prime la norme qui la précède » (15). Cette règle de priorité est fondée sur l'idée selon laquelle le législateur tient compte du cadre normatif en vigueur lorsqu'il impose une nouvelle disposition légale ou réglementaire. Partant, si cette dernière est incompatible avec celles qui lui sont chronologiquement antérieures, il faut y voir une volonté du législateur de modifier en conséquence le cadre normatif. Selon nous, l'application de cet adage est secondaire et ne doit intervenir que lorsque l'autre règle de priorité ne permet pas d'apporter de solution satisfaisante. En effet, on peut supposer que s'il souhaite qu'une hypothèse donnée, déjà régie par une disposition particulière, soit soumise à un régime distinct, le législateur veille à abroger la loi la plus ancienne ou à établir expressément une priorité entre les normes. S'il ne le fait pas, c'est qu'il juge les régimes complémentaires, dans certains cas. Il est donc *a priori* justifié de les maintenir.

---

(13) X. DIJON, *Méthodologie juridique. L'application de la norme*, Diegem, Kluwer, 1996, p. 95, n° 313.

(14) Voy. P. DELNOY, *Précis de méthodologie juridique,* 2e éd., Bruxelles, Larcier, 2006, p. 382, n° 118 : « parfois, le législateur règle d'une certaine manière une catégorie générique de faits et, d'une autre manière, une des espèces appartenant à ce genre. Dans ce cas, s'il se vérifie que les faits concernés présentent toutes les caractéristiques qui permettent de les classer sous le concept spécifique, on doit leur appliquer la seconde règle, en vertu du principe : *specialia generalibus derogant* ».

(15) X. DIJON, *op. cit.,* p. 95, n° 313.

2. Vue panoramique et générale de l'articulation entre le RGPD, d'une part, le DSA et DORA, d'autre part

2.1. RGPD et DSA

7. Objet du DSA. Le règlement sur les services numériques a pour objet d'encadrer la fourniture de certains services intermédiaires au sein du marché intérieur, soit les activités de simple transport, de mise en cache et d'hébergement, y compris, dans ce dernier cas, les plateformes en ligne (16). Les très grandes plateformes en ligne (VLOP) et les très grands moteurs de recherche en ligne (VLOSE) sont également visés, et débiteurs d'obligations additionnelles. En fonction du risque qu'ils présentent, pour les citoyens et les entreprises de l'Union, les services visés par le règlement (et les prestataires qui les fournissent), sont soumis à des exigences plus ou moins nombreuses et contraignantes.

Le DSA est entré en application le 17 février 2024 (17).

Le règlement encadre ainsi la responsabilité des prestataires intermédiaires, en déterminant notamment dans quelles hypothèses, et moyennant le respect de quelles conditions, ils bénéficient d'une exonération totale ou partielle de responsabilité. Diverses mesures permettant de lutter contre les contenus illicites sont également adoptées (avec la mise en place d'un mécanisme de notification et d'action, par exemple). Des obligations de transparence et de loyauté sont aussi prévues, en particulier pour lutter contre les *dark patterns* ou garantir la traçabilité des professionnels dans les contrats à distance B2C. La publicité et d'autres pratiques promotionnelles (profilage, recommandations, etc.) font également l'objet de règles plus strictes. Dans ces domaines, les VLOP et les VLOSE sont soumis à des obligations renforcées et nettement plus sévères.

De manière générale, le DSA s'applique aux services intermédiaires (18), soit les services de la société de l'information (19) (i) de simple transport, (ii) de « mise en cache » ou (iii) d'hébergement (20). Dans ce dernier cas de figure, on vise entre autres les réseaux sociaux, les plateformes de stockage dans le cloud, les places de marché en ligne ou les sites de partage de contenus. Pour le reste, peu importe l'objet ou la nature des services fournis à travers la plateforme en ligne ou l'un des trois services intermédiaires : vente ou location de biens, fourniture de services (et/ou, le cas échéant, de contenus ou de services numériques), dans le domaine de la mobilité, du droit, de l'art, de la santé, de l'éducation, de la banque, de l'assurance, etc. Le champ d'application personnel est large également, puisque le destinataire du service peut être une personne morale ou une personne physique, intervenant à des fins

(16) Pour un commentaire du DSA, voy. M. LEDGER et A. MICHEL, « Règlement (UE) 2022/2065 sur les services numériques (règlement sur les services numériques – « Digital Services Act ») », *R.D.T.I.*, 2023/92-93, pp. 124 et s.

(17) Art. 93 du DSA. Il était déjà applicable aux très grandes plateformes en ligne et aux très grands moteurs de recherche en ligne depuis le 25 août 2023 (art. 92 du DSA).

(18) Définis à l'art. 3, g), du DSA.

(19) Définis à l'art. 3, a), du DSA, qui renvoie à la définition figurant à l'art. 1 (1), point b), de la directive (EU) 2015/1535.

(20) Ces trois notions sont définies à l'art. 3, g), du DSA (de manière identique à ce que prévoyait la directive sur le commerce électronique).

professionnelles ou non (21). Des règles plus contraignantes sont toutefois prescrites lorsque le destinataire est un consommateur. Enfin, et c'est un élément capital pour garantir l'effectivité du règlement, les fournisseurs de services intermédiaires sont soumis à celui-ci même s'ils ne sont pas établis sur le territoire de l'Union européenne (22). S'agissant du champ d'application spatial, il s'applique en effet « aux services intermédiaires proposés aux destinataires de services dont le lieu d'établissement est situé dans l'Union ou qui sont situés dans l'Union » (23).

8. Dans quels cas le DSA et le RGPD devraient-ils être appliqués de manière simultanée dans le domaine des assurances ? Les compagnies d'assurances ou les intermédiaires d'assurances ne devraient normalement pas être considérés comme des prestataires de services intermédiaires au sens du DSA (24). Leurs services ne peuvent en effet pas être considérés comme du simple transport, de la mise en cache ou de l'hébergement.

Par contre, ils devraient régulièrement être en contact avec des fournisseurs de tels services, en tant que clients professionnels, par exemple pour héberger certaines de leurs données dans le cloud, pour faire de la publicité sur des réseaux sociaux ou des moteurs de recherche, voire encore pour demander le retrait de contenus considérés comme illicites (des informations mensongères, par exemple).

Dans ce contexte, et sauf exception, l'articulation avec le RGPD ne devrait pas poser de difficulté particulière : les règles matérielles de celui-ci devraient au contraire compléter utilement celles du DSA.

C'est notamment le cas en matière de publicité lorsque, conformément à l'article 26, § 3, du DSA, « les fournisseurs de plateformes en ligne ne présentent pas aux destinataires du service de publicité qui repose sur du profilage, tel qu'il est défini à l'article 4, point 4), du règlement (UE) 2016/679, en utilisant les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679 ».

Confirmant cette complémentarité, l'article 2, § 4, g), du DSA énonce que celui-ci s'entend sans préjudice des règles établies par d'autres actes juridiques de l'Union, parmi lesquels figure logiquement le RGPD (25).

(21) *Cf.* la définition large du destinataire du service à l'art. 3, b).

(22) Dans ce cas, ils doivent désigner un représentant légal dans un Etat membre de l'UE (art. 13 du DSA).

(23) Art. 2, § 1er, du DSA.

(24) Voy. en ce sens l'article 2, § 2, du DSA, suivant lequel « le présent règlement ne s'applique pas aux services qui ne sont pas des services intermédiaires ou aux exigences imposées à l'égard de tels services, que ces services soient ou non fournis par le biais d'un service intermédiaire ».

(25) Il est intéressant de noter que la directive 2000/31/CE sur le commerce électronique règle l'articulation entre les textes de manière différente. L'article 1er, § 5, de cette directive énonce en effet qu'elle n'est pas applicable « aux questions relatives aux services de la société de l'information couvertes par les directives 95/46/CE et 97/66/CE », ce qui établit une priorité au bénéfice des directives encadrant les traitements de données à caractère personnel.

2.2. RGPD et DORA

9. Objet de DORA. Le recours sans cesse croissant au numérique par les entités du secteur financier expose celles-ci aux cybermenaces (26), de plus en plus nombreuses et sophistiquées. Parallèlement, l'infrastructure ou le matériel IT ne sont pas à l'abri des dysfonctionnements ou d'une mauvaise utilisation. Des risques évidents en résultent, non seulement pour les acteurs directement impliqués (et leurs clients), mais également pour la société dans son ensemble, avec une possible perte de confiance dans les marchés financiers et les institutions (27).

S'agissant spécialement du secteur des assurances, le considérant n° 2 de DORA note que celui-ci « a également été transformé par l'utilisation des TIC avec l'apparition des intermédiaires d'assurance offrant des services en ligne et fonctionnant avec les technologies du domaine de l'assurance (InsurTech) ou la souscription d'assurance. L'ensemble du secteur financier a non seulement opéré une transition vers le numérique à grande échelle, mais la numérisation a également renforcé les interconnexions et les relations de dépendance au sein du secteur financier et avec les prestataires tiers d'infrastructures et de services ».

DORA entend apporter des réponses à ces enjeux de cybersécurité, en mettant en place des règles harmonisées visant à garantir la résilience opérationnelle numérique des entités financières (28). L'expression désigne « la capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations » (29).

DORA sera applicable à partir du 17 janvier 2025 (30).

Les entités financières, telles que listées à l'article 2, § 1er, du règlement sont soumises à celui-ci. Dans le secteur qui nous occupe, sont visées les entreprises d'assurance et de réassurance (point n), d'une part, les intermédiaires d'assurance, les intermédiaires de réassurance et les intermédiaires d'assurance à titre accessoire (point o), d'autre part. Des exceptions sont toutefois prévues, notamment pour les intermédiaires d'assurance et de réassurance qui sont par ailleurs des microentreprises, des petites ou des moyennes entreprises (31).

(26) L'expression désigne « toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes » (art. 3, 12), de DORA, qui renvoie à l'art. 2, point 8), du règlement (UE) 2019/881).

(27) *Cf.* le considérant n° 3 de DORA.

(28) Pour un commentaire, voy. M. SCHELLEMANS et E. KUN, « Cyberresilience in the Financial Sector: Overall Analysis of the Digital Operational Resilience Act", *R.D.T.I.*, 2023/92-93, pp. 100 et s.

(29) Art. 3, 1), de DORA.

(30) Art. 64 de DORA.

(31) Art. 2, § 3, de DORA.

Dans le respect du principe de proportionnalité (32), diverses mesures doivent être prises par les entités financières : gestion du risque lié aux TIC (33) ; gestion, classification et notification des incidents liés aux TIC (34) ; tests de résilience opérationnelle numérique (35) et gestion des risques liés aux prestataires tiers de services TIC (36). L'article 45 du règlement encourage également le partage d'informations et de renseignement sur les cybermenaces par les entités financières.

10. Application conjointe de DORA et du RGPD dans le domaine des assurances ? De manière générale, DORA ne traite pas expressément de l'articulation entre ses dispositions et celles du RGPD (37). Le règlement ne contient d'ailleurs aucune disposition établissant une priorité éventuelle par rapport au RGPD ou indiquant qu'il s'applique « sans préjudice » de celui-ci. Les deux instruments devraient donc s'appliquer de manière cumulative (38).

Pourtant, en pratique, les points de convergence devraient être nombreux : les risques et incidents liés aux TIC ou résultant de l'intervention des prestataires tiers peuvent en effet concerner les données à caractère personnel des clients des compagnies d'assurances et des intermédiaires, susceptibles d'être détruites, altérées ou de faire l'objet d'un *data breach*. Sans prétendre à l'exhaustivité, on pointe dans les lignes qui suivent quelques exemples de ces convergences.

Conformément au RGPD, diverses obligations reposent ainsi sur le responsable du traitement et le sous-traitant, en termes de sécurité des (traitements de) données à caractère personnel. Pour les satisfaire, ils doivent mettre en œuvre « des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques », et qui comprennent notamment « a) la pseudonymisation et le chiffrement des données à caractère personnel ; b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement » (39).

On trouve des exigences similaires, quoique nettement plus développées, dans DORA (outre qu'elles s'appliquent également à d'autres objets que les seules don-

(32) Art. 4 de DORA.
(33) Chap. II du règlement, art. 5 et s.
(34) Chap. III du règlement, art. 17 et s.
(35) Chap. IV du règlement, art. 24 et s.
(36) Chap. V du règlement, art. 28 et s.
(37) Des références ponctuelles sont toutefois faites à cet instrument, notamment dans le cadre des dispositifs de partage d'informations et de renseignements sur les cybermenaces (art. 45, § 1er, c), de DORA) et pour les traitements de données des autorités européennes de surveillances et les autorités compétentes (art. 56 de DORA).
(38) M. SCHELLEMANS et E. KUN, « Cyberresilience in the Financial Sector: Overall Analysis of the Digital Operational Resilience Act », *R.D.T.I.*, 2023/92-93, p. 104, n° 223.
(39) Art. 32, § 1er, du RGPD.

nées). Parmi d'autres, on peut ainsi reprendre les dispositions de l'article 9 de ce règlement, §§ 2 et 3 :

« les entités financières conçoivent, acquièrent et mettent en œuvre des stratégies, des politiques, des procédures, des protocoles et des outils de sécurité de TIC qui visent à garantir la résilience, la continuité et la disponibilité des systèmes de TIC, en particulier ceux qui soutiennent des fonctions critiques ou importantes, et à maintenir des normes élevées en matière de disponibilité, d'authenticité, d'intégrité et de confidentialité des données, que ce soit au repos, en cours d'utilisation ou en transit.

Pour atteindre les objectifs visés au paragraphe 2, les entités financières utilisent des solutions et des processus de TIC qui sont appropriés conformément à l'article 4. Ces solutions et processus de TIC : a) garantissent la sécurité des moyens de transfert de données ; b) réduisent au minimum le risque de corruption ou de perte de données, d'accès non autorisé et de défauts techniques susceptibles d'entraver les activités ; c) empêchent le manque de disponibilité, les atteintes à l'authenticité et à l'intégrité, les violations de la confidentialité et la perte de données ; d) garantissent que les données sont protégées contre les risques découlant de la gestion des données, y compris une mauvaise administration, les risques relatifs au traitement et l'erreur humaine » (40).

Conformément au RGPD, une analyse d'impact relative à la protection des données doit également être réalisée dans certains cas (41), ce qui requiert d'anticiper les risques et de prendre les mesures qui s'imposent pour les prévenir. Les principes de protection des données dès la conception (*by design*) et par défaut (*by default*) participent de ce même objectif. Les nombreuses exigences relatives à la gestion des risques liés aux TIC (42), en termes de gouvernance et de prévention notamment, prévues par DORA, partagent cette même finalité.

Des exigences de notification sont prévues par le RGPD en cas de violation des données à caractère personnel (43). DORA encadre également les procédures de gestion des incidents liés aux TIC, notamment en prescrivant des obligations de notification (44). Si de tels événements surviennent, les compagnies d'assurances ou les intermédiaires devront par conséquent se soumettre à ces procédures, vis-à-vis des autorités compétentes au titre de chaque instrument (dont on espère qu'elles veilleront à collaborer (45)) et, le cas échéant, à l'égard des personnes concernées.

La relation contractuelle entre le responsable du traitement et son sous-traitant (qui peut être un prestataire tiers de services TIC au sens de DORA) est également encadrée par le RGPD (46), qui impose d'y indiquer, notamment, les mesures techniques et organisationnelles envisagées conformément à l'article 32. Parallèlement, le sous-traitant ne peut être choisi que s'il présente des « garanties suffisantes quant à la

(40) Voy. aussi l'art. 12 de DORA relatif aux politiques et procédures de sauvegarde, ainsi qu'aux procédures et méthodes de rétablissement.
(41) Art. 35 du RGPD.
(42) Art. 6 et s. de DORA.
(43) Art. 33 et 34 du RGPD.
(44) Art. 17 et s. de DORA.
(45) En ce sens, M. SCHELLEMANS et E. KUN, « Cyberresilience in the Financial Sector: Overall Analysis of the Digital Operational Resilience Act", *R.D.T.I.*, 2023/92-93, pp. 104-105.
(46) Art. 28 du RGPD.

mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée » (47). Les relations contractuelles entre les entités financières et les prestataires de services TIC sont également encadrées de manière stricte par les articles 28 et suivants de DORA (spécialement au moment d'évaluer et de choisir ces prestataires, et relativement au contenu des obligations contractuelles à convenir). Il en résulte que les conventions conclues entre les compagnies d'assurances et leurs cocontractants, fournisseurs de technologies, devront respecter les obligations imposées sur ce point par le RGPD et par DORA.

Les exigences prévues par DORA en termes de cybersécurité étant particulièrement strictes et détaillées, leur respect permettra généralement aux entités financières de s'en prévaloir au moment de démontrer que leurs obligations corrélatives, prévues par le RGPD en termes de sécurité, ont été observées. A l'inverse, sauf si les compagnies d'assurances ou les intermédiaires avaient mis en place des procédures extrêmement strictes pour se soumettre aux exigences du RGPD en termes de sécurité (ou à d'autres dispositions légales ou réglementaires applicables), ils devront remettre l'ouvrage sur le métier pour s'assurer du respect des nouvelles obligations imposées par DORA.

3. Focus sur l'articulation entre le RGPD, d'une part, le DA et l'AIA, d'autre part

3.1. Articulation du Data Act avec le RGPD

11. Objet du *Data Act*. Le *Data Act* (48) (ou DA), adopté le 13 décembre 2023 (et qui sera applicable, sauf exception, à partir du 12 septembre 2025 (49)), a notamment pour but d'établir des règles portant sur le partage de données dans le domaine de l'Internet des objets (« *Internet of Things* » ou « *IoT* ») (50). Plus précisément, le

(47) Art. 28, § 1er, du RGPD. Dans son avis sur la proposition de règlement, le CEPD insiste sur le respect des exigences en matière de transferts internationaux de données, lorsque le prestataire est dans un pays tiers (CEPD, Avis n° 7/2021 du 10 mai 2021 sur la proposition de règlement sur la résilience opérationnelle numérique du secteur financier et modifiant les règles (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014 et (UE) n° 909/2014, p. 8).

(48) Règlement (UE) 2023/2854 du Parlement européen et du Conseil concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données), *J.O.*, L, 22 décembre 2023. Pour une synthèse du *Data Act*, voy. C. ANTOINE, « Règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données – « *Data Act* ») », *R.D.T.I.*, 2023/92-93, pp. 34-57.

(49) Art. 50 du DA.

(50) Voy. art. 3 et s. du DA. D'autres objectifs – qui vont au-delà de l'objet du présent propos – sont poursuivis par le DA, à savoir (i) la mise à disposition de données au profit des organismes du secteur public, de la Commission, de la Banque centrale européenne et des organes de l'Union en cas de besoin exceptionnel de disposer de ces données pour exécuter une mission spécifique d'intérêt public, (ii) l'introduction de garanties contre l'accès et le transfert internationaux illicites de données à caractère non personnel par les autorités publiques, (iii) la facilitation du passage d'un service de traitement de données à un autre, ou encore (iv) le développement de normes d'interopérabilité pour les espaces de données (art. 1er, § 1er, du DA).

DA vise à imposer au détenteur de données (51) de partager certaines données avec l'utilisateur (52) d'un produit connecté (53) – tel qu'une montre ou une voiture connectée – ou d'un service connexe (54) (55) – par exemple, un logiciel utilisé pour traiter les données enregistrées par une montre ou une voiture connectée – ou, le cas échéant, de les mettre à disposition du tiers désigné par cet utilisateur. Ces obligations imposées au détenteur de données pourraient être perçues comme conférant à l'utilisateur un « droit d'accès » et un « droit à la portabilité des données » de portée spécifique.

12. Délimitation et plan du propos. Le présent propos se concentre sur l'articulation entre les dispositions du DA en matière de partage de données dans le domaine de l'Internet des objets et le RGPD, en particulier ses articles 15 et 20, qui reconnaissent aux personnes concernées un droit d'accès et un droit à la portabilité des données. Nous examinons d'abord les données visées par ces dispositions (3.1.1.), puis les droits d'accès (3.1.2.) et à la portabilité des données (3.1.3.) prévus par le DA et, enfin, les limites posées à ces droits (3.1.4.).

(51) Le détenteur de données est « […] une personne physique ou morale qui, conformément au présent règlement, aux dispositions applicables du droit de l'Union ou à la législation nationale adoptée conformément au droit de l'Union, a le droit ou l'obligation d'utiliser et de mettre à disposition des données, y compris, lorsqu'il en a été convenu par contrat, des données relatives au produit ou des données relatives au service connexe qu'elle a extraites ou générées au cours de la fourniture d'un service connexe » (art. 2, 13), du DA). Il y a lieu de préciser que, sous certaines conditions, le détenteur de données n'est pas soumis aux obligations de mise à disposition des données s'il est considéré comme une microentreprise, une petite entreprise ou une moyenne entreprise (voy. art. 7, § 1er, du DA).

(52) L'utilisateur est « […] une personne physique ou morale à laquelle appartient un produit connecté ou à laquelle des droits temporaires d'utilisation de ce produit connecté ont été cédés contractuellement, ou qui reçoit des services connexes » (art. 2, 12), du DA).

(53) Un produit connecté est « […] un objet qui obtient, génère ou recueille des données concernant son utilisation ou son environnement, qui est en mesure de communiquer des données relatives au produit par l'intermédiaire d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré et dont la fonction première n'est pas de stocker, de traiter ou de transmettre des données pour le compte de toute partie autre que l'utilisateur » (art. 2, 5), du DA).

(54) Un service connexe est défini comme « […] un service numérique, autre qu'un service de communications électroniques, y compris un logiciel, qui est connecté au produit au moment de l'achat, ou de la mise en location ou en crédit-bail, de telle sorte que son absence empêcherait le produit connecté d'exécuter une ou plusieurs de ses fonctions, ou qui est ensuite connecté au produit par le fabricant ou un tiers pour ajouter, mettre à jour ou adapter les fonctions du produit connecté » (art. 2, 6), du DA).

(55) Sont aussi visés les assistants virtuels qui interagissent avec un produit connecté ou un service connexe (art. 1er, § 4, du DA). Au sens du DA, les assistants virtuels sont « […] des logiciels capables de traiter des demandes, des tâches ou des questions, notamment celles fondées sur des données d'entrée sonores ou écrites, ou des gestes ou des mouvements, et qui, sur la base de ces demandes, tâches ou questions, donnent accès à d'autres services ou contrôlent les fonctions des produits connectés » (art. 2, 31), du DA).

3.1.1. Données visées

13. Données relatives au produit et au service connexe. Les données (56) concernées par les obligations de mise à disposition prévues par le DA sont :

(i) les données relatives au produit, définies comme « […] les données générées par *l'utilisation d'un produit connecté* que le fabricant a *conçu pour qu'elles puissent être extraites*, au moyen d'un service de communications électroniques, d'une connexion physique ou d'un dispositif d'accès intégré, par un utilisateur, un détenteur de données ou un tiers, y compris, le cas échéant, le fabricant » (57) ; et

(ii) les données relatives au service connexe, définies comme « […] les données représentant la *numérisation des actions de l'utilisateur ou des événements liés au produit connecté, enregistrées intentionnellement par l'utilisateur ou générées en tant que produit annexe de l'action de l'utilisateur* lors de la fourniture d'un service connexe par le fournisseur » (58).

14. Données non substantiellement modifiées et données prétraitées. Aux termes du considérant n° 15 du DA, sont uniquement concernées par les obligations de mise à disposition les « données qui ne sont pas substantiellement modifiées » (59) (« données sources/primaires ») et les « données qui ont été prétraitées dans le but de les rendre compréhensibles et utilisables avant leur traitement et leur analyse ultérieurs » (60).

Inversement, sont exclues du champ d'application de ces obligations de mise à disposition les informations déduites ou dérivées des données précitées, résultant soit d'investissements supplémentaires dans l'attribution de valeurs, soit d'informations tirées de ces données, par application d'algorithmes propriétaires complexes, par exemple (61).

15. Données facilement accessibles. Le DA ajoute encore que, lorsqu'une demande d'accès ou de portabilité des données est introduite par l'utilisateur, seules les données facilement accessibles et les métadonnées (62) pertinentes nécessaires pour les interpréter et les utiliser doivent être partagées. Les données facilement ac-

(56) Les données consistent en « […] toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels » (art. 2, 1), du DA). Les données ne peuvent cependant constituer du « contenu » (voy. à cet égard le cons. 16 et l'art. 1er, § 2, a), du DA).

(57) Art. 2, 15), du DA (nous soulignons).

(58) Art. 2, 16), du DA (nous soulignons).

(59) Il s'agit « […] des points de données qui sont générés automatiquement sans autre forme de traitement […] » (cons. 15 du DA).

(60) « […] Ces données comprennent les données collectées à partir d'un capteur unique ou d'un groupe de capteurs connecté dans le but de rendre les données collectées compréhensibles pour les cas d'utilisation plus larges en déterminant une grandeur ou une qualité physique ou la modification d'une grandeur physique, telle que la température, la pression, le débit, l'audio, la valeur de pH, le niveau de liquide, la position, l'accélération ou la vitesse […] » (cons. 15 du DA).

(61) « […] Ces données pourraient comprendre en particulier les informations obtenues au moyen de la fusion de capteurs, qui infère ou déduit des données provenant de capteurs multiples, collectées dans le produit connecté, au moyen d'algorithmes complexes et propriétaires, et qui pourraient être soumises à des droits de propriété intellectuelle » (cons. 15 du DA).

(62) Les métadonnées sont définies comme « […] une description structurée du contenu ou de l'utilisation des données qui facilite la découverte ou l'utilisation de ces données » (art. 2, 2), du DA).

cessibles sont définies comme les « […] données relatives à un produit et les données relatives à un service connexe qu'un détenteur de données obtient légalement ou peut obtenir légalement à partir du produit connecté ou du service connexe, sans effort disproportionné allant au-delà d'une simple opération » (63).

16. Données à caractère personnel et à caractère non personnel. Les données couvertes par les obligations de mise à disposition prévues par le DA peuvent être tant des données à caractère personnel – auquel cas, en principe, le RGPD trouvera également à s'appliquer – que des données à caractère non personnel (64).

Une donnée à caractère personnel est définie 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 » (65).

Comme le précise le considérant n° 26 du RGPD, ne sont pas considérées comme des « données à caractère personnel » les informations anonymes et les données à caractère personnel rendues anonymes. Une donnée anonyme suppose que la personne physique à laquelle elle se rapporte ne soit pas identifiable. L'évaluation du caractère « identifiable » de la personne – qui est loin d'être un exercice aisé – implique la prise en compte de « […] 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 […] », étant entendu que « […] [p]our 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* […] » (66).

Conformément à la jurisprudence de la Cour de justice de l'Union européenne (CJ), il apparaît qu'une donnée peut être considérée comme anonyme lorsque le risque d'identification de la personne à laquelle elle se rapporte paraît insignifiant en raison de l'effort démesuré – en termes de main-d'œuvre, de coût et de temps, par

(63) Art. 2, 17), du DA. Des précisions sont apportées par le considérant n° 20 du DA : « […] [o]n entend par "données facilement accessibles" les données relatives au produit et au service connexe qu'un détenteur de données obtient ou peut obtenir légalement du produit connecté ou du service connexe, *par exemple au moyen de la conception du produit connecté, du contrat passé entre le détenteur de données et l'utilisateur pour la fourniture de services connexes et des moyens techniques d'accès aux données dont le détenteur de données dispose, sans effort disproportionné*. Les données facilement accessibles ne comprennent pas les données générées par l'utilisation d'un produit connecté lorsque la conception du produit connecté ne prévoit pas que ces données sont stockées ou transmises en dehors du composant dans lequel elles sont générées ou du produit connecté dans son ensemble » (nous soulignons).

(64) Il s'agit des « […] données autres que les données à caractère personnel » (art. 2, 4), du DA).

(65) Art. 4, 1), du RGPD (voy. art. 2, 3), du DA).

(66) Cons. 26 du RGPD (nous soulignons).

exemple – qu'impliquerait cette identification (67). Cette jurisprudence semble ainsi suggérer qu'une évaluation du risque de réidentification de la personne concernée devrait être réalisée pour déterminer si une donnée doit ou non être qualifiée de « donnée à caractère personnel » (68). A l'instar de la position adoptée par A. Gobert, M. Knockaert, M. Rappe et J.-M. Van Gyseghem, nous estimons que « […] [cette] approche va également de pair avec l'application d'un critère "relatif" au moment de déterminer quelles sont les personnes à même de déployer les moyens raisonnables. En appliquant ce critère, il est possible de considérer que des données sont à caractère personnel vis-à-vis d'un premier organisme, mais ne le sont pas vis-à-vis d'un second qui ne disposerait pas des informations supplémentaires nécessaires à l'identification de la personne concernée sans efforts démesurés […] » (69).

17. Illustration : voitures connectées et assurances « *Pay How You Drive* ». A titre illustratif, nous faisons référence aux voitures connectées et aux assurances auto de type « *Pay As You Drive* » (PHYD) (70) (71). Il s'agit d'assurances auto dont le montant des primes est fixé en fonction de la manière dont la voiture assurée est conduite. Plus l'assuré

(67) C.J., arrêt *OC c. Commission européenne*, 7 mars 2024, aff. C-479/22 P, EU:C:2024:215, points 51 et 63 ; C.J., arrêt *Patrick Breyer c. Bundesrepublik Deutschland*, 19 octobre 2016, aff. C-582/14, EU:C:2016:779, point 46 ; T.U.E., arrêt *Conseil de résolution unique (CRU) c. Contrôleur européen de la protection des données (CEPD)*, 26 avril 2023, aff. T-557/20, EU:T:2023:219, point 93.

(68) En ce sens : A. Gobert, M. Knockaert, M. Rappe et J.-M. Van Gyseghem, « La donnée à caractère personnel et sa réutilisation », *J.T.*, 2024, n° 8, pp. 125-126. Comme l'expliquent ces auteurs, certains défendent quant à eux une approche dite « risque zéro » en vertu de laquelle une donnée ne peut être considérée comme anonyme que s'il n'existe aucun risque – ou presqu'aucun risque – d'identification de la personne à laquelle elle se rapporte.

(69) *Ibidem*, p. 125. *A contrario*, les partisans de l'approche dite « risque zéro » défendent l'application d'un critère « objectif » selon lequel une donnée revêt un caractère personnel dès qu'une personne dispose d'informations qui, en combinaison avec cette donnée, rendent possible l'identification de la personne à laquelle la donnée se rapporte (*ibidem*, p. 125). À notre sens, la Cour de justice s'est prononcée en faveur de l'application du critère relatif dans son arrêt *Gesamtverband Autoteile-Handel eV c. Scania CV AB* : « […] une donnée telle que le VIN – qui est défini par l'article 2, point 2, du règlement n° 19/2011 comme un code alphanumérique attribué au véhicule par son constructeur, afin d'assurer l'identification adéquate de ce véhicule et qui, en tant que tel, est dépourvu de caractère "personnel" – *acquiert ce caractère* ***à l'égard de*** *quiconque dispose raisonnablement de moyens permettant de l'associer à une personne déterminée* » (C.J., arrêt *Gesamtverband Autoteile-Handel eV c. Scania CV AB*, 9 novembre 2023, aff. C-319/22, EU:C:2023:837, point 46 – nous soulignons).

(70) Dans certains pays, par exemple aux Etats-Unis, en Inde et au Royaume-Uni, des compagnies d'assurances permettent à leurs clients d'opter pour une assurance auto de type « PHYD ». A l'heure actuelle, l'offre en la matière semble inexistante en Belgique. AG Insurance s'y est toutefois intéressée en 2015 lorsqu'elle a mené un projet pilote consistant à équiper les voitures de membres de son personnel d'une boîte noire pour analyser leur comportement au volant. Elle a conclu que le déploiement d'assurances PHYD sur le marché belge n'était pas indiqué (en 2016) et que des études approfondies en la matière se révélaient nécessaires (AG Insurance, « Boîtes noires – un test riche en enseignements, mais une étude approfondie est nécessaire », 29 février 2016, disponible sur : https://newsroom.aginsurance.be/test-boites-noires/, consulté le 30 avril 2024).

(71) Il y a lieu de faire mention d'une initiative européenne portant spécifiquement sur les conditions d'accès et d'utilisation des données générées à bord des véhicules et pouvant notamment viser des services tels que les réparations et entretiens, la mobilité en tant que service, le partage de véhicules et les assurances. Cette initiative semble être en suspens depuis la consultation publique ayant eu lieu du 29 mars au 2 août 2022 (Commission européenne, « Accès aux données, aux fonctions et aux ressources des véhicules », *s.d.*, disponible sur : https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Acces-aux-donnees-aux-fonctions-et-aux-ressources-des-vehicules_fr, consulté le 10 mai 2024).

est un « conducteur prudent », plus le montant des primes est avantageux (72). Pour pouvoir fixer le montant de la prime, la compagnie d'assurances utilise un logiciel traitant toute une série de données relatives à la voiture et au comportement du conducteur, par exemple le kilométrage, la localisation, la vitesse, les données liées à l'accélération et au freinage ou encore la durée et la fréquence de déplacement (73). A l'heure actuelle, le recours à ces données et leur traitement semblent de plus en plus aisés eu égard, d'une part, à la diversité et au volume de données que peut générer une voiture connectée et, d'autre part, aux performances croissantes des outils d'intelligence artificielle (IA) (74).

Dans le cadre de ce type d'assurance, les différents types de données pouvant être traités par les compagnies d'assurances consistent à la fois en des données relatives au produit – la voiture connectée – et en des données relatives au service connexe – le logiciel traitant les données enregistrées par la voiture connectée. Dans la plupart des cas, il semble qu'il s'agisse de données à caractère personnel, en ce compris les données de nature technique (75). Toutes ces données sont en principe liées à l'assuré (ou à la personne renseignée comme conducteur de la voiture si l'assuré n'en est pas conducteur (76)) et permettent donc à la compagnie d'assurances d'identifier la personne à laquelle elles se rapportent. Toutefois, le caractère « personnel » de ces données pourrait être discuté si la voiture était utilisée par d'autres personnes que l'assuré ou la personne renseignée comme conducteur auprès de la compagnie d'assurances. Dans cette hypothèse, la compagnie d'assurances serait amenée à traiter des données relatives à des personnes qu'elle ne pourrait *a priori* identifier. Selon nous, par application du critère relatif défini ci-avant (77), il convient de déterminer

(72) Toutefois, dans certains cas, l'assuré considéré comme un « conducteur prudent » ne voit pas le montant de ses primes diminuer, mais se voit accorder d'autres avantages tels que la possibilité de ne pas payer de suppléments s'il parcourt plus de kilomètres que le plafond couvert par sa police d'assurance (Association of British Insurers (ABI), « 'Pay How You Drive' Motor Insurance », avril 2013, disponible sur : https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/migrated/telematics/pay-how-you-drive-motor-insurance---abi-consumer-guide.pdf, consulté le 30 avril 2024).

(73) R. MAHESHWARI, « Pay As You Drive Insurance: Meaning And Benefits », *Forbes Advisor*, 8 mars 2024, disponible sur : https://www.forbes.com/advisor/in/car-insurance/pay-as-you-drive-insurance/#:~:text=Both%20Pay%20As%20You%20Drive,one%20is%20driving%20their%20vehicle, consulté le 3 mai 2024.

(74) Cela ne signifie toutefois pas que le déploiement de ce type d'assurance est nécessairement « acceptable » pour la société. En outre, il devrait s'accompagner d'un respect strict du cadre réglementaire existant, au premier chef le RGPD (voy. spéc. art. 5, §1er, c), 6 et 22). Pour une analyse de l'assurance PHYD au prisme du droit à la protection de la vie privée et des données à caractère personnel, voy. 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 », *For. ass.*, 2017/173, pp. 75-83.

(75) Comme l'indique le Comité européen de la protection des données (EDPB), « […] la plupart des données associées aux véhicules connectés sont considérées comme des données à caractère personnel dans la mesure où il est possible de les associer à une ou plusieurs personnes identifiables. Il s'agit notamment des données techniques relatives aux mouvements du véhicule (par exemple, la vitesse, la distance parcourue) ainsi qu'à l'état du véhicule (par exemple, la température du liquide de refroidissement, le régime du moteur, la pression des pneus) […] » (EDPB, « Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés et des applications liées à la mobilité », version 2.0, 9 mars 2021, point 62). Voy. également : J. METZGER et D. GILL, « Data Access Through Data Portability. Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars », *E.D.P.L.*, 2022/2, p. 226.

(76) Pensons notamment à l'hypothèse dans laquelle l'assuré serait une personne morale, par exemple l'employeur du conducteur.

(77) Voy. *supra*, n° 16.

au cas par cas si ces données revêtent ou non un caractère personnel à l'égard de la compagnie d'assurances en réalisant une évaluation du risque d'identification à la lumière des principes dégagés par la CJ (78).

3.1.2. Droit d'accès

18. Droit d'accès de l'utilisateur d'un produit connecté ou d'un service connexe. Le DA permet à l'utilisateur d'avoir accès aux données relatives au produit et au service connexe. A cette fin, le DA prévoit tout d'abord un principe que l'on pourrait qualifier d'« accessibilité des données dès la conception » (79) selon lequel « [l]es produits connectés sont *conçus et fabriqués*, et les services connexes *conçus et fournis*, de telle sorte que les données relatives auxdits produits et les données relatives aux services connexes, y compris les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données, sont, par défaut, accessibles à l'utilisateur, de manière aisée, sécurisée, sans frais, *dans un format complet, structuré, couramment utilisé et lisible par machine, et sont, lorsque cela est pertinent et techniquement possible, directement accessibles à l'utilisateur* » (80).

Si l'utilisateur ne peut accéder directement aux données – en raison de l'absence de pertinence de cette accessibilité directe aux données et/ou de son impossibilité technique (81) –, il peut adresser une demande d'accès au détenteur de données. Lorsque c'est techniquement possible, cette demande doit être envoyée par voie électronique (82). Le détenteur des données devra alors mettre à la disposition de l'utilisateur sans retard injustifié, gratuitement, aisément, de manière sécurisée et dans un format structuré, complet, lisible par machine et couramment utilisé les données facilement accessibles et les métadonnées pertinentes nécessaires pour les interpréter et les utiliser. Elles doivent en outre avoir un niveau de qualité identique à celui dont dispose le détenteur de données. Par ailleurs, si c'est pertinent et techniquement possible, ces données et métadonnées devront être rendues accessibles à l'utilisateur en continu et en temps réel (83).

19. Demande d'accès portant sur des données à caractère personnel relatives à un tiers. Il se peut que les données relatives au produit et/ou au service connexe soient des données à caractère personnel concernant un tiers à l'utilisateur. Dans ce cas, le détenteur de données pourrait anonymiser les données en question (84) ou, dans l'hypothèse où les données sont relatives à plusieurs personnes concernées, en ce compris l'utilisateur, ne mettre à disposition de celui-ci que les données à caractère personnel le concernant (85). S'il ne procède pas de la sorte, le détenteur de données ne pourra partager les données avec l'utilisateur que si le traitement de données qui en résulte est fondé sur l'une des bases de licéité énumérées à l'article 6 du RGPD ou à l'article 9 du RGPD (si les données concernées sont des données

(78) Il convient toutefois de souligner qu'en pratique, il semble particulièrement compliqué d'un point de vue technique de distinguer précisément les données relatives à l'assuré (ou à la personne renseignée comme conducteur) des données relatives à d'autres personnes qui conduiraient la voiture concernée.

(79) C. ANTOINE, *op. cit.*, p. 41.

(80) Art. 3, § 1er, du DA (nous soulignons).

(81) Le DA n'apporte toutefois pas de précisions quant à la portée de ces notions.

(82) Art. 4, § 1er, du DA.

(83) Art. 4, § 1er, du DA

(84) Concernant la problématique de l'anonymisation, nous renvoyons à ce qui a été exposé *supra* (voy. n° 16).

(85) Cons. 7 du DA.

sensibles). Il devra en outre vérifier, le cas échéant, si les conditions prévues par l'article 5, § 3, de la directive *e-Privacy* (86) sont satisfaites (87).

20. Comparaison avec le droit d'accès consacré par le RGPD. Le tableau ci-dessous offre une comparaison de la portée du droit d'accès prévu par le DA, d'une part, du droit d'accès reconnu par le RGPD, d'autre part.

	DA (art. 3 et 4)	**RGPD (art. 15)**
Émetteur de la demande	Utilisateur	Personne concernée
Destinataire de la demande	Détenteur de données	Responsable du traitement
Données visées	Données facilement accessibles Métadonnées pertinentes nécessaires à l'utilisation et à l'interprétation de ces données	Données à caractère personnel Informations relatives au traitement(88)
Modalités d'introduction de la demande	Par voie électronique lorsque c'est techniquement possible	Absence d'exigences particulières
Coût	Aucun coût	Principe : aucun coût Exception : possibilité pour le responsable du traitement d'exiger le paiement de frais raisonnables sur la base des coûts administratifs supportés en cas de demande de copie supplémentaire par la personne concernée ou de demandes manifestement infondées ou excessives(89)
Délai de réponse	« sans retard injustifié »	Au plus tard un mois à compter de la réception de la demande (possibilité de prorogation de deux mois selon la complexité et le nombre de demandes)(90)
Exigences applicables	Mise à disposition des données de manière aisée et sécurisée et dans un format structuré, complet, lisible par machine et couramment utilisé Lorsque c'est pertinent et techniquement possible : accessibilité en continu et en temps réel	Si la demande est introduite par voie électronique : fourniture des informations sous une forme électronique d'usage courant (sauf en cas de contre-indication de la personne concernée)

Tableau 1. Droit d'accès : comparaison DA – RGPD

(86) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.*, L 201, 31 juillet 2022. L'article 5, § 3, de la directive *e-Privacy* établit les conditions à remplir pour utiliser un réseau de communications électroniques afin de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un utilisateur ou d'un abonné.

(87) Art. 4, § 12, du DA.

(88) Voy. art. 15, §§ 1er-2, du RGPD.

(89) Art. 12, § 5, a), du RGPD.

(90) Art. 12, § 3, du RGPD.

21. Articulation avec le droit d'accès consacré par le RGPD. Si l'utilisateur est une personne concernée au sens du RGPD, il jouit, selon nous, tant du droit d'accès prévu par le DA que du droit d'accès consacré par le RGPD (91). Ces deux droits doivent être perçus comme complémentaires, comme le précise l'article 1er, § 5, du DA : « […] [d]ans la mesure où les utilisateurs sont des personnes concernées, les droits prévus au chapitre II du présent règlement complètent les droits d'accès des personnes concernées et les droits à la portabilité des données au sens des articles 15 et 20 du [RGPD] […] ».

3.1.3. Droit à la portabilité des données

22. Droit à la portabilité des données de l'utilisateur d'un produit connecté ou d'un service connexe. Le droit à la portabilité des données prévu par le DA permet à l'utilisateur ou à une partie agissant pour le compte de celui-ci (92) de demander au détenteur de données de mettre à la disposition d'un tiers les données facilement accessibles et les métadonnées pertinentes nécessaires à l'interprétation et à l'utilisation de ces données. Cette mise à disposition des données au tiers doit se faire dans les mêmes conditions que celles applicables à une demande d'accès (93). Toutefois, dans les relations entre entreprises, le détenteur de données doit par ailleurs convenir avec le tiers – s'il s'agit d'un destinataire de données au sens du DA (94) – des modalités de mise à disposition des données de manière transparente et en appliquant des conditions équitables, raisonnables et non discriminatoires (95), y compris en ce qui concerne la compensation applicable (96). Il y a toutefois lieu de souligner que si un accord quant aux modalités de mise à disposition des données n'est pas trouvé, l'exercice des droits conférés à la personne concernée par le RGPD – en particulier son droit à la portabilité des données – ne peut être entravé (97).

23. Exceptions à l'exercice du droit à la portabilité des données. Le droit à la portabilité des données ne peut être exercé dans deux situations :

(i) lorsque les données facilement accessibles sont relatives à de nouveaux produits connectés, procédés ou substances n'ayant pas encore été mis sur le marché et étant soumis à des essais, à moins que l'utilisation de ces données par un tiers soit permise contractuellement (98) ;

---

(91) A cet égard, voy. *infra*, n° 26.

(92) Par exemple, le tiers avec lequel l'utilisateur souhaite partager les données.

(93) Art. 5, § 1er, du DA. Voy. *supra*, n° 18.

(94) Le tiers sera qualifié de « destinataire de données » s'il s'agit d'« […] une personne physique ou morale, autre que l'utilisateur d'un produit connecté ou d'un service connexe, agissant à des fins qui sont liées à son activité commerciale, industrielle, artisanale ou libérale, à la disposition duquel le détenteur de données met des données, y compris un tiers lorsque l'utilisateur a adressé une demande au détenteur de données ou conformément à une obligation légale découlant du droit de l'Union ou de la législation nationale adoptée conformément au droit de l'Union » (art. 2, 14), du DA).

(95) Art. 8, § 1er, du DA. A cet égard, il y a lieu d'ajouter qu'un régime de clauses abusives entre entreprises est instauré par le DA et doit donc être pris en compte lors de la négociation des modalités de mise à disposition des données (voy. art. 13 du DA).

(96) Art. 9, § 1er, du DA. Pour des précisions quant à la fixation d'une compensation raisonnable et non discriminatoire, voy. art. 9 et cons. 46 à 51. Il convient notamment d'indiquer que la Commission est chargée d'adopter des lignes directrices relatives au calcul d'une compensation raisonnable.

(97) Art. 5, § 8, du DA.

(98) Art. 5, § 2, du DA.

(ii) lorsque le tiers avec lequel les données sont destinées à être partagées est un contrôleur d'accès (*gatekeeper*) au sens du Règlement (UE) 2022/1925 sur les marchés numériques (*Digital Markets Act*) (99) (100).

24. Demande de portabilité portant sur des données à caractère personnel relatives à un tiers (renvoi). Si la demande de portabilité concerne des données relatives à un tiers à l'utilisateur, les mêmes exigences que celles relatives aux demandes d'accès sont applicables (101).

25. Comparaison avec le droit à la portabilité des données consacré par le RGPD. Le tableau ci-dessous propose une vue comparative de la portée du droit à la portabilité des données tel que visé par le DA et du droit à la portabilité des données prévu par le RGPD.

	DA (art. 5)	**RGPD (art. 20)**
Émetteur de la demande	Utilisateur ou partie agissant pour le compte de celui-ci	Personne concernée
Destinataire de la demande	Détenteur de données	Responsable du traitement
Données visées	Données facilement accessibles, sauf si elles sont relatives à de nouveaux produits connectés, procédés ou substances n'ayant pas encore été mis sur le marché et étant soumis à des essais (à moins que l'utilisation de ces données par un tiers soit permise contractuellement) Métadonnées pertinentes nécessaires à l'utilisation et à l'interprétation de ces données	Données à caractère personnel fournies par la personne concernée au responsable du traitement
Conditions spécifiques	Qualité du tiers : pas un contrôleur d'accès (*gatekeeper*)	Base de licéité du traitement : consentement (art. 6, § 1er, a), ou art. 9, § 2, a)) ou contrat (art. 6, § 1er, b)) Traitement effectué à l'aide de procédés automatisés
Modalités d'introduction de la demande	Absence d'exigences particulières	Absence d'exigences particulières

(99) Règlement (UE) 2022/1925 du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques), *J.O.*, L 265, 12 octobre 2022.

(100) Art. 5, § 3, du DA. Le DA interdit également toute mise à disposition des données aux contrôleurs d'accès qui résulterait de l'exercice par l'utilisateur de son droit d'accès ou de son droit à la portabilité des données au bénéfice d'un tiers (art. 5, § 3, et art. 6, § 2, d), du DA).

(101) Art. 5, § 7, du DA. Voy. *supra*, n° 19.

	DA (art. 5)	RGPD (art. 20)
Coût	Aucun coût pour l'utilisateur Compensation due par le tiers au détenteur de données	Principe : aucun coût Exception : possibilité pour le responsable du traitement d'exiger le paiement de frais raisonnables sur la base des coûts administratifs supportés en cas de demandes manifestement infondées ou excessives(102)
Délai de réponse	« sans retard injustifié »	Au plus tard un mois à compter de la réception de la demande (possibilité de prorogation de deux mois selon la complexité et le nombre de demandes)(103)
Exigences applicables	Mise à disposition des données de manière aisée et sécurisée et dans un format structuré, complet, lisible par machine et couramment utilisé Lorsque c'est pertinent et techniquement possible : accessibilité en continu et en temps réel Dans les relations entre entreprises : conclusion d'un accord portant sur les modalités de mise à disposition des données avec le tiers de manière transparente et en appliquant des conditions équitables, raisonnables et non discriminatoires (y compris concernant la compensation applicable)	Mise à disposition dans un format structuré, lisible par machine et couramment utilisé

Tableau 2. Droit à la portabilité des données : comparaison DA – RGPD

26. Articulation avec le droit à la portabilité des données consacré par le RGPD. Si l'utilisateur est une personne concernée, le droit à la portabilité des données prévu par le DA doit être vu comme complémentaire au droit à la portabilité des données reconnu par le RGPD (104).

Comme le résume le considérant n° 35 du DA, « […] [l']article 20 du [RGPD] indique qu'il porte sur les *données fournies* par la personne concernée, mais ne précise pas si cela nécessite un comportement actif de la part de la personne concernée ou s'il s'applique également aux situations dans lesquelles un produit connecté ou un service connexe, par sa conception, observe le comportement d'une personne concernée ou d'autres informations relatives à une personne concernée de manière passive. […] Le [DA] accorde aux utilisateurs le droit d'accéder à toutes données relatives à un produit ou données relatives à un service connexe et de mettre celles-ci à la disposition d'un tiers, quelle que soit leur nature en tant que données à caractère personnel, *sans distinction entre les données fournies activement et les données observées passivement*, *et quelle que soit la base juridique du traitement* […] » (105).

(102) Art. 12, § 5, a), du RGPD.
(103) Art. 12, § 3, du RGPD.
(104) Art. 5, § 1er, du DA.
(105) Nous soulignons.

Il est vrai que les contours de la notion de « données fournies » ne sont pas clairement définis par le RGPD (106). Comme l'indiquent J. Metzger et D. Gill, cette notion peut être interprétée de manière étroite ou de manière large. Si l'on optait pour une interprétation étroite, seules les données activement et sciemment fournies par la personne concernée pourraient être couvertes par une demande de portabilité au sens du RGPD. Il s'agirait par exemple des données liées à un compte utilisateur communiquées via un formulaire en ligne. Si, en revanche, l'interprétation large devait être suivie, le droit à la portabilité des données pourrait en outre s'appliquer aux « données observées » – données découlant de l'observation des interactions et activités de la personne concernée – ainsi qu'aux « données déduites » – qui sont dérivées ou déduites des données fournies activement par la personne concernée ou des données observées (107). Le Groupe de travail « Article 29 » sur la protection des données (G29) adopte une position intermédiaire qui couvre les données observées (par exemple, les données brutes traitées par des objets connectés, l'historique d'utilisation d'un site web, des activités de recherche ou des journaux d'activités), mais pas les données déduites telles que le résultat d'une appréciation concernant la santé d'un utilisateur ou un profil créé dans le cadre d'une réglementation financière ou d'une réglementation relative à la gestion des risques (108). Le DA semble adopter une approche similaire dès lors qu'aux termes de son 15e considérant, le droit à la portabilité des données ne couvre que les données non substantiellement modifiées et les données prétraitées, à l'exclusion des informations déduites ou dérivées de ces données (109).

En définitive, dans le domaine de l'Internet des objets, il semble que le droit à la portabilité des données prévu par le DA ait une portée matérielle plus large que celui prévu par le RGPD dès lors qu'il couvre (i) tant les données à caractère personnel que les données à caractère non personnel, (ii) les données observées (dont on ne peut pas affirmer avec certitude qu'elles sont couvertes par le droit à la portabilité des données consacré par le RGPD, bien que cette interprétation soit la plus plausible eu égard à l'avis du G29), (iii) les données dont le traitement est fondé sur une autre base de licéité que le consentement ou le contrat et (iv) les métadonnées perti-

(106) Voy. not. S. Toropainen, « The right to data portability in the fair data economy – extending the right of individuals to benefit from managing their data », 6 septembre 2023, pp. 15-17, disponible sur : https://helda.helsinki.fi/items/46635581-9dc3-4fe1-a231-f5fb6ee0c9ea.

(107) J. Metzger et D. Gill, *op. cit.*, p. 226.

(108) Selon le G29, « […] [e]n général, compte tenu des objectifs stratégiques du droit à la portabilité des données, l'expression "fournies par la personne concernée" doit être interprétée au sens large, et devrait exclure les "données déduites" et les "données dérivées", qui incluent les données à caractère personnel qui sont créées par un prestataire de services (par exemple, des résultats algorithmiques). Un responsable du traitement peut exclure ces données déduites, mais doit inclure toutes les autres données à caractère personnel fournies par la personne concernée via les moyens techniques mis à disposition par le responsable du traitement. Par conséquent, l'expression "fournies par" englobe les données à caractère personnel qui se rapportent à l'activité de la personne concernée ou qui résultent de l'observation du comportement d'une personne, mais exclut les données résultant d'une analyse subséquente de ce comportement. En revanche, les données à caractère personnel qui ont été créées par le responsable du traitement dans le cadre du traitement des données, par exemple, par un processus de personnalisation ou de recommandation, par catégorisation ou profilage des utilisateurs, sont des données qui sont dérivées ou déduites des données à caractère personnel fournies par la personne concernée et elles ne sont pas couvertes par le droit à la portabilité des données […] » (G29, « Lignes directrices relatives au droit à la portabilité des données », WP 242 rev.01, 5 avril 2017, pp. 12-13).

(109) Voy. *supra*, n° 14.

nentes nécessaires à l'utilisation et à l'interprétation des données mises à disposition. Afin de pouvoir partager avec un tiers un plus large éventail de données, l'utilisateur qui a la qualité de personne concernée préférera dès lors exercer le droit à la portabilité qui lui est reconnu par le DA plutôt que par le RGPD. Certains auteurs semblent toutefois considérer que lorsque des données à caractère personnel sont concernées, seul le droit à la portabilité des données reconnu par le RGPD pourrait être exercé, le DA ne pouvant être perçu comme une « *lex specialis* » (110).

Nous ne partageons toutefois pas cet avis. Une telle interprétation viendrait considérablement réduire l'effet utile du DA et ne semble pas, à notre sens, refléter la volonté du législateur. Cela ressort principalement de l'article 1er, § 5, du DA, qui identifie comme complémentaires les droits d'accès et à la portabilité des données prévus par le DA, d'une part, par le RGPD, d'autre part, et du libellé du considérant n° 35 du DA (111) (112). La circonstance que le DA prévoie expressément que les dispositions du RGPD prévalent en cas de conflit (113) ne permet pas, selon nous, de conclure le contraire. En effet, le droit à la portabilité des données prévu par le DA ne semble pas en conflit avec le droit à la portabilité des données reconnu par le RGPD. Le premier a simplement une portée plus large que le second dans le domaine de l'Internet des objets. En outre, l'introduction de cette clause de hiérarchie dans le DA semble avoir pour but d'éviter toute mauvaise interprétation des dispositions du DA qui créerait un risque de violation du RGPD dans la situation où l'utilisateur, qui ne serait pas une personne concernée au sens du RGPD, serait amené à traiter des données à caractère personnel (114). La raison d'être de cette clause de

(110) S. Toropainen, *op. cit.*, p. 19. En ce sens : D. Spajic et T. Lalova-Spinks, « The broadening of the right to data portability for IoT products: Who does the Act actually empower? », *in White Paper on the Data Act Proposal*, C. Ducuing, Th. Margoni et L. Schirru (dir.), 26 octobre 2022, p. 31, disponible sur : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4259428.

(111) Aux termes du considérant n° 35 du DA : « […] Le [DA] accorde aux utilisateurs le droit d'accéder à toutes données relatives à un produit ou données relatives à un service connexe et de mettre celles-ci à la disposition d'un tiers, quelle que soit leur nature en tant que données à caractère personnel, *sans distinction entre les données fournies activement et les données observées passivement*, *et quelle que soit la base juridique du traitement* […] » (nous soulignons).

(112) En ce sens : Th. Tombal et I. Graef, « The Regulation of Access to Personal and Non-personal Data in the EU: From Bits and Pieces to a System? », *TILEC Discussion Paper*, n° 2022-019, novembre 2022, p. 13, disponible sur : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4304148.

(113) Art. 5, § 1er, du DA.

(114) Cela ressort de l'avis conjoint 2/2022 de l'EDPB et du Contrôleur européen de la protection des données (CEPD) : « [l]'EDPB et le CEPD reconnaissent que d'autres entités que la personne concernée peuvent avoir une raison légitime d'accéder aux données générées par l'utilisation d'un produit ou d'un service lié. Parallèlement, ils estiment qu'il existe également un risque important que les droits d'accès, de partage ou d'utilisation des données générées par l'utilisation d'un produit ou d'un service lié soient exercés de manière à porter indûment atteinte aux droits et libertés des personnes concernées. À titre d'illustration, un employeur qui a acheté des assistants vocaux virtuels et les a mis à la disposition de ses employés pourrait utiliser le droit d'accès pour accéder à l'historique de leurs recherches. […] Afin de limiter les risques d'une interprétation ou d'une mise en œuvre de la proposition susceptible d'entacher ou de compromettre l'application de la législation existante en matière de protection des données, l'EDPB et le CEPD appellent les co-législateurs à renforcer la formulation de l'article 1, paragraphe 3, en précisant explicitement qu'en cas de conflit avec les dispositions de la proposition, la législation en matière de protection des données "**prévaut**" pour autant qu'elle concerne le traitement des données à caractère personnel » (Avis conjoint 2/2022 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), 4 mai 2022, points 25-26).

hiérarchie n'est donc pas de faire prévaloir le droit à la portabilité des données consacré par le RGPD sur celui prévu par le DA.

27. Illustration : voitures connectées et assurances PHYD. Dans le cadre du déploiement d'une assurance PHYD, l'exercice par l'assuré – en sa qualité d'utilisateur – du droit à la portabilité des données au profit de la compagnie d'assurances – destinataire de données – semble constituer un moyen efficace de partager les données générées par le véhicule connecté, d'autant plus si ces données peuvent être partagées en continu et en temps réel (115). En pratique, la compagnie d'assurances pourrait, après avoir reçu l'autorisation de l'utilisateur et sous réserve du respect du RGPD, directement s'adresser au détenteur de données – qui serait en principe le constructeur automobile (116) – dès lors que la demande de portabilité peut être introduite par une partie agissant pour le compte de l'utilisateur (117). Un accord portant sur les modalités de mise à disposition des données, y compris sur la compensation due au détenteur de données, devrait ensuite être conclu entre la compagnie d'assurances et le détenteur de données. Comme indiqué ci-avant, si les parties ne parviennent pas à s'entendre sur les modalités d'un tel accord, l'utilisateur qui est une personne concernée pourra toujours exercer son droit à la portabilité des données en vertu du RGPD (118).

3.1.4. Limites aux droits d'accès et à la portabilité des données

28. Limites aux droits d'accès et à la portabilité des données. Certaines limites à l'exercice des droits d'accès et à la portabilité des données sont prévues par le DA et doivent dès lors être prises en compte dans le cadre de l'éventuelle mise en œuvre de ces droits dans le secteur des assurances :

(i) en cas de risque d'atteinte aux exigences légales de sécurité du produit connecté entraînant de graves effets indésirables pour la sécurité, la santé ou la sûreté de personnes physiques, des limitations contractuelles portant sur l'accès aux données, leur utilisation ou leur partage ultérieur peuvent être prévues (119) ;

(ii) si l'exercice des droits d'accès et à la portabilité des données peut porter atteinte aux secrets d'affaires du détenteur de données ou d'un tiers, des mesures destinées à préserver la confidentialité de ces secrets d'affaires doivent être mises en place (120) ;

(iii) l'exercice des droits d'accès et à la portabilité des données ne peut avoir pour but de permettre à l'utilisateur ou à un tiers de développer un produit connecté concurrent (121) ou d'obtenir des informations concernant la situation écono-

(115) Pour rappel, cette exigence est d'application « lorsque c'est pertinent et techniquement possible » (art. 5, § 1er, du DA).

(116) J. METZGER et D. GILL, *op. cit.*, p. 226.

(117) Art. 5, § 1er, du DA.

(118) Art. 5, § 8, du DA. La portée de ce droit paraît toutefois plus réduite que celle du droit à la portabilité des données reconnu par le DA (voy. *supra*, n° 26).

(119) Art. 4, § 2, du DA.

(120) Art. 4, § 6 et art. 5, § 9, du DA. Dans certaines circonstances liées à la préservation de la confidentialité des secrets d'affaires, le détenteur de données pourra, selon le cas, rejeter la demande de mise à disposition de données qu'il reçoit ou bloquer ou suspendre le partage de données (voy. art. 4, §§ 7-8 et art. 5, §§ 10-11, du DA).

(121) Art. 4, § 10, et art. 6, § 2, e), du DA. Pour des précisions à propos de cette interdiction, voy. cons. 32 du DA.

mique, les méthodes de production ou les actifs du fabricant ou du détenteur de données (122) ;

(iv) pour accéder aux données, l'utilisateur et le tiers ne peuvent ni recourir à des moyens coercitifs ni tirer profit des lacunes qui seraient présentes dans l'infrastructure technique mise en place par le détenteur de données pour protéger les données (123).

3.2. Articulation de l'AI Act avec le RGPD

29. Objet et présentation générale de l'AI Act. Conformément à l'article 1er, § 1er, de l'AI Act, « l'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur et de promouvoir l'adoption d'une intelligence artificielle (IA) axée sur l'humain et digne de confiance, tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte, notamment la démocratie, l'état de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation ».

Sauf exception, il sera applicable à partir du 2 août 2026 (124).

Le règlement distingue plusieurs catégories de systèmes d'IA (125), soumises à des règles plus ou moins strictes en fonction du risque (126) qu'ils créent (127).

Certaines pratiques en matière d'IA, listées à l'article 5 du règlement, sont ainsi purement et simplement interdites (sauf exceptions) en raison des risques jugés inacceptables qui en résultent : sont notamment visés les systèmes qui exploitent les vulnérabilités dues à l'âge ou au handicap et qui sont susceptibles de causer un préjudice important, les systèmes de *social scoring*, voire encore ceux qui visent à prédire la probabilité de la commission d'une infraction pénale sur la base du profilage d'une personne.

La deuxième catégorie regroupe les systèmes d'IA à haut risque. Un tel système est ainsi qualifié (i) lorsqu'il constitue un produit (ou le composant de sécurité d'un produit) visé par l'un des textes énoncés à l'annexe I et relatifs, par exemple, à l'aviation civile, aux véhicules à moteur, aux jouets, aux ascenseurs ou aux dispositifs médicaux (128) ou (ii) lorsque, sauf exceptions (129), il est visé à l'annexe III (130). Celle-ci mentionne plusieurs secteurs dans lesquels des systèmes d'IA sont susceptibles d'être utilisés

(122) Art. 4, § 10 et art. 6, § 2, e), du DA.
(123) Art. 4, § 11 et art. 5, § 5, du DA.
(124) Art. 113 de l'AIA.
(125) Voy. l'art. 3, 1), de l'AIA pour la définition du « système d'IA » : « un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels ».
(126) La notion est définie à l'article 3, 2), du AIA et désigne « la combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci ».
(127) Voy. Commission européenne, "Artificial Intelligence - Questions and Answers", 1er août 2024, pp. 2 et s.
(128) Art. 6, § 1er, de l'AIA.
(129) Art. 6, § 3, de l'AIA.
(130) Art. 6, § 2, de l'AIA.

(éducation et formation professionnelle, emploi, répression, administration de la justice, etc.). En matière d'assurance, on peut notamment relever le point 5, c), de l'annexe relatif « aux systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-vie et d'assurance maladie ». De nombreuses conditions, particulièrement strictes et détaillées, doivent être respectées : le règlement énumère ainsi les exigences applicables aux systèmes d'IA à haut risque (131) (établissement d'un système de gestion des risques, documentation technique, enregistrement automatique des événements, transparence, contrôle humain, etc.) ; les obligations incombant aux fournisseurs, aux déployeurs ainsi qu'à d'autres parties, comme les importateurs ou les distributeurs (132) (notamment en termes d'évaluation de la conformité par des organismes tiers avant la mise sur le marché ou la mise en service) ; le rôle joué par les autorités notifiantes et les organismes d'évaluation de la conformité (133), ainsi que les règles relatives aux normes harmonisées, aux spécifications communes, aux certificats établis par les organismes notifiés, à la déclaration UE de conformité, au marquage CE et à l'enregistrement dans la base de données de l'UE (134). Le but de ces règles est de garantir qu'au moment de leur mise sur le marché, les systèmes d'IA présentent le niveau de sécurité attendu et qu'ils pourront être utilisés sans risque : dans une logique de « *compliance* », le règlement IA intervient en amont, pour que seuls les systèmes d'IA à haut risque conformes aux normes adoptées puissent être mis sur le marché et utilisés.

La troisième catégorie regroupe les systèmes d'IA qui présentent un risque spécifique en matière de transparence. On vise par exemple les chatbots mis en place par les entreprises pour donner des renseignements aux clients. Ces systèmes sont principalement soumis à des obligations d'information, pour permettre aux personnes physiques de savoir qu'elles interagissent avec une machine (et qu'elles puissent décider de poursuivre la discussion ou pas) ou pour marquer clairement les contenus ou les résultats générés ou manipulés par une IA (135).

Enfin, les systèmes d'IA présentant un risque minimal (un filtre anti-spam, par exemple) peuvent être mis sur le marché et utilisés librement. Aucune exigence particulière n'est imposée par l'AI Act, qui se borne à promouvoir l'élaboration de codes de conduites en la matière (136).

A côté de cette classification, construite à la lumière des applications possibles des systèmes d'IA (et des risques corrélatifs), une autre typologie est établie, fondée sur la technologie sous-jacente. L'AI Act établit en effet des règles applicables aux modèles d'IA à usage général (137), en distinguant ceux qui présentent un risque systé-

(131) Art. 8 et s. de l'AIA.
(132) Art. 16 et s. de l'AIA.
(133) Art. 28 et s. de l'AIA.
(134) Art. 40 et s. de l'AIA.
(135) Art. 50 de l'AIA.
(136) Art. 95 de l'AIA.
(137) La notion est définie à l'art. 3, 63), de l'AIA. Elle désigne « un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché ».

mique (138) et les autres (139). Cette partie a été ajoutée au cours du processus législatif, pour répondre aux enjeux posés par les IA génératives telles que ChatGPT ou Copilot. Les modèles d'IA à usage général sont généralement intégrés dans des systèmes d'IA (avec d'autres composantes importantes). Dans la suite de la contribution, nous nous focaliserons principalement sur les systèmes d'IA.

30. Traitements de données à caractère personnel dans le cadre de l'AI Act et renvoi au RGPD. S'agissant de textes de portée transversale, dont le champ d'application est particulièrement large, le RGPD et l'AI Act devraient régulièrement être appliqués de manière simultanée : les systèmes d'IA doivent en effet être entraînés sur des données (qui peuvent être à caractère personnel) et leur finalité est très souvent de produire du contenu ou de dégager des solutions en lien avec des personnes physiques identifiées ou identifiables.

L'article 2, § 7, de l'AIA énonce ainsi que « le droit de l'Union en matière de protection des données à caractère personnel, de respect de la vie privée et de confidentialité des communications s'applique aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement. Le présent règlement n'a pas d'incidence sur le règlement (UE) 2016/679 ou le règlement (UE) 2018/1725, ni sur la directive 2002/58/CE ou la directive (UE) 2016/680, sans préjudice de l'article 10, paragraphe 5, et de l'article 59 du présent règlement » (140).

Les deux corpus réglementaires doivent par conséquent être respectés en parallèle, chacun en ce qui le concerne (141).

L'AI Act contient d'ailleurs diverses références aux traitements de données et aux conditions à respecter dans ce cadre, spécialement pour les systèmes d'IA à haut risque. La déclaration de conformité UE applicable à ceux-ci conformément à l'article 47 du règlement doit ainsi contenir l'information suivante : « lorsqu'un système d'IA nécessite le traitement de données à caractère personnel, une déclaration qui atteste que ledit système d'IA est conforme aux règlements (UE) 2016/679 et (UE) 2018/1725 ainsi qu'à la directive (UE) 2016/680 » (142).

Quant au RGPD, même s'il précède l'AI Act de plusieurs années, il règle déjà les décisions fondées exclusivement sur les traitements automatisés (dans lesquelles

(138) La notion de risque systémique est définie à l'art. 3, 65), de l'AIA.

(139) Art. 51 et s. de l'AIA.

(140) S'agissant de l'article 10, § 5, voy. *infra*, n° 32. Quant à l'article 59 du règlement IA, il figure dans le chapitre relatif aux mesures de soutien à l'innovation et permet un traitement ultérieur de données à caractère personnel dans le cadre du bac à sable réglementaire de l'IA, pour d'autres fins que celles pour lesquelles elles ont été collectées, moyennant le respect de plusieurs conditions cumulatives : préserver des intérêts publics importants, critère de nécessité, protection par des mesures techniques et organisationnelles, etc.

(141) Conformément au cons. n° 10 de l'AIA, « le présent règlement n'entend pas modifier l'application du droit de l'Union régissant le traitement des données à caractère personnel, ni les tâches et les pouvoirs des autorités de contrôle indépendantes chargées de veiller au respect de ces instruments ».

(142) Annexe V, point 5, du règlement IA.

des systèmes d'IA seront généralement mobilisés), tout en posant divers principes généraux également applicables en la matière (143).

Des difficultés d'articulation ne sont pas à exclure, notamment lorsque la non-conformité du système d'IA est à l'origine d'un *data breach* ou de traitements de données donnant lieu à des biais ou des discriminations (intervention potentielle d'autorités compétentes distinctes ; obligations de notification spécifiques à chaque instrument, etc.). S'agissant de l'articulation entre le droit financier et le droit de l'IA, le considérant n° 138 de l'AIA encourage la désignation des autorités compétentes dans le secteur financier pour la surveillance de la mise en oeuvre du règlement.

Nous reviendrons sur l'articulation entre les deux textes, en distinguant la collecte et l'entraînement des données, d'une part, les décisions prises à l'égard de personnes physiques au moyen d'une IA, d'autre part (*infra*, n° 32).

31. Quelle démarche les compagnies d'assurances doivent-elles entreprendre si elles utilisent l'IA ? Les applications potentielles de l'intelligence artificielle dans le domaine des assurances sont nombreuses et variées : pour détecter les fraudes, calculer une prime, évaluer un risque, automatiser certains processus contractuels, répondre aux questions fréquentes des utilisateurs dans un chatbot, etc.

D'un point de vue méthodologique, les compagnies d'assurances (ou les intermédiaires, le cas échéant) devront d'abord classer le système d'IA utilisé dans l'une des quatre catégories visées précédemment, en déterminant leur rôle, en tant que « fournisseur » (144) et/ou comme « déployeur » (145) du système d'IA, et en articulant celui-ci avec la qualification en tant que responsable du traitement ou sous-traitant au sens du RGPD.

L'utilisation d'un chatbot devrait ainsi relever de la catégorie 3 (risque spécifique en matière de transparence – outre qu'il constituera normalement un système d'IA à usage général au sens de l'article 3, 66), tandis que les systèmes d'IA mobilisés dans les assurances-crédits pour évaluer la solvabilité des personnes physiques (146), ou dans les assurances-vie et les assurances maladies à des fins d'évaluation des risques et de tarification (147), expressément mentionnés à l'Annexe III, doivent être considérés à haut risque. Le considérant n° 58 du règlement le justifie par le fait que ces systèmes d'IA « peuvent avoir une incidence significative sur les moyens

(143) A ce sujet, voy. A. DELFORGE et L. GÉRARD, « Notre vie privée est-elle réellement mise en danger par les robots ? Etudes des risques et analyse des solutions apportées par le GDPR », *L'intelligence artificielle et le droit,* Bruxelles, Larcier, 2017, pp. 143 et s.

(144) La notion est définie à l'art. 3, 3), de l'AIA et désigne « une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit ».

(145) La notion est définie à l'art. 3, 4), de l'AIA et désigne « une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel ».

(146) Voy. le point 5, b), de l'Annexe III, répertoriant les systèmes d'IA à haut risque visés par l'article 6, § 2, de l'AIA.

(147) Voy. le point 5, c), de l'Annexe III, répertoriant les systèmes d'IA à haut risque visés par l'article 6, § 2, de l'AIA.

de subsistance de ces personnes et, s'ils ne sont pas dûment conçus, développés et utilisés, peuvent porter atteinte à leurs droits fondamentaux et entraîner de graves conséquences pour leur vie et leur santé, y compris l'exclusion financière et la discrimination ». Ce même considérant ajoute cependant que « les systèmes d'IA prévus par le droit de l'Union aux fins de détecter les fraudes dans l'offre de services financiers et à des fins prudentielles pour calculer les besoins en fonds propres des établissements de crédit et des compagnies d'assurance ne devraient pas être considérés comme étant à haut risque au titre du présent règlement ». La finalité du système devra donc être analysée avec précision.

Le fournisseur pourrait également démontrer que, même s'il est visé à l'Annexe III, le système n'est pas à haut risque : le paragraphe 3 de l'article 6 prévoit en effet que tel est le cas « lorsqu'il ne présente pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques, y compris en n'ayant pas d'incidence significative sur le résultat de la prise de décision ». L'une des quatre conditions énumérées à l'alinéa 2 devra également être satisfaite, par exemple quand la finalité du système d'IA est d'accomplir une tâche procédurale étroite (détecter des doublons, par exemple) ou à améliorer le résultat d'une activité humaine préalablement réalisée (améliorer la manière dont le document est rédigé, par exemple) (148).

Qu'en est-il de l'assurance « *Pay how you drive* », dont la tarification aurait été établie par une IA, sur la base des données recueillies relativement au comportement du conducteur ? L'hypothèse ne crée pas un risque inacceptable et le système ne devrait donc pas être interdit purement et simplement. S'agit-il d'un système d'IA à haut risque ? Il ne figure pas dans la liste des hypothèses visées à l'Annexe III. Il pourrait toutefois être considéré comme tel s'il est le composant de sécurité d'un produit (ou un produit en tant que tel) couvert par les textes de l'Annexe I. Dans l'exemple, on peut avoir égard au règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route. Ce texte ne vise toutefois pas spécifiquement l'hypothèse de l'enregistrement des données à caractère personnel des utilisateurs en vue d'une analyse ultérieure par une IA à des fins de tarification (149) ; on peut aussi arguer que, dans ce cas, le recours à l'IA ne pose pas de risque en termes de sécurité du produit (ce qui n'exclut pas les atteintes potentielles à la vie privée, les discriminations ou l'exclusion financière). En cas d'interaction directe avec la personne physique concernée, il s'agira d'un système d'IA présentant un risque spécifique en matière de transparence et soumis aux obligations d'information de l'article 50 du règlement IA. Les exigences prescrites par l'AI Act devraient donc être relativement réduites. D'autres obligations pourraient toutefois être applicables : on songe notamment à l'article 22 du RGPD (à ce sujet, voy. *infra*, n° 33).

32. Données à caractère personnel traitées dans le cadre de l'entraînement de l'IA. Les systèmes d'intelligence artificielle se nourrissent de données. Si celles-ci

(148) Voy. le cons. n° 52 de l'AIA.

(149) L'enregistrement des données d'événement est expressément visé (art. 6, § 1er, g), du règlement 2019/2144) mais il est soumis à des prescriptions très strictes et n'est *a priori* pas destiné aux compagnies d'assurance dans une perspective de tarification (art. 6, § 4, du règlement 2019/2144).

sont anonymes (à ce sujet, voy. *supra*, n° 16), le RGPD ne trouvera pas à s'appliquer. Pour les données à caractère personnel, par contre, une couche additionnelle de règles devra être observée. Le respect des principes posés par le RGPD pourrait d'ailleurs être particulièrement délicat dans un contexte de big data (on pense notamment aux principes de limitation des finalités et de minimisation des données (150)).

L'article 10 du règlement IA, intitulé « Données et gouvernance des données », énonce quant à lui, en son paragraphe 1er, que « les systèmes d'IA à haut risque faisant appel à des techniques qui impliquent l'entraînement de modèles d'IA au moyen de données sont développés sur la base de jeux de données d'entraînement, de validation et de test qui satisfont aux critères de qualité visés aux paragraphes 2 à 5 chaque fois que ces jeux de données sont utilisés ». En fonction des données utilisées, des discriminations ou des biais peuvent en effet être créés. Le paragraphe 5 de la disposition autorise d'ailleurs les fournisseurs des systèmes d'IA à haut risque à traiter, exceptionnellement, des catégories particulières de données à caractère personnel (au sens de l'article 9 du RGPD (151) – origine raciale ou ethnique, convictions religieuses, données de santé, etc.), dans la mesure où c'est strictement nécessaire pour détecter et corriger les biais. L'article 9, § 1er, du RGPD interdit en effet les traitements portant sur ces catégories particulières de données à caractère personnel, sauf si l'une des conditions du § 2 est satisfaite. Vu les enjeux en termes de droits fondamentaux, plusieurs conditions additionnelles sont posées par le règlement IA : proportionnalité, mise en place de limitations techniques relatives à la réutilisation des données, pas de communication par d'autres parties, suppression dès que le biais a été corrigé, justification dans le registre, etc.

Conformément à l'AI Act, une attention particulière doit également être apportée à la collecte des données à caractère personnel et à la finalité de celles-ci (152).

33. Comment articuler l'article 22 du RGPD avec les dispositions de l'AI Act ? Depuis 2018, en cas de recours à des systèmes d'intelligence artificielle, il convient d'établir si l'article 22 du RGPD est d'application et, dans l'affirmative, si les conditions qu'il prévoit pour lever l'interdiction sont réunies.

Aux termes de cette disposition, « la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire » (153). Les trois conditions prescrites par cette

(150) Art. 5, § 1er, b) et c), du RGPD. A ce sujet, voy. H. JACQUEMIN et J.-M. VAN GYSEGHEM, « Le big data en matière d'assurance à l'épreuve du RGPD », *Bull. Ass.*, dossier 2017, *Data Protection : l'impact du GDPR en assurances*, pp. 233-260.

(151) Art. 3, 37), de l'AIA.

(152) Art. 10, § 2, b), de l'AIA : « les jeux de données d'entraînement, de validation et de test sont soumis à des pratiques en matière de gouvernance et de gestion des données appropriées à la destination des systèmes d'IA à haut risque. Ces pratiques concernent en particulier : […] b) les processus de collecte de données et l'origine des données, ainsi que, dans le cas des données à caractère personnel, la finalité initiale de la collecte de données ».

(153) Sur cette disposition, voy. Th. TOMBAL, « Les droits de la personne concernée dans le R.G.P.D. », *Le règlement général sur la protection des données (RGPD/GDPR). Analyse approfondie,* Coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 531 et s. ; G. REGOUT, « Assurances : le profilage et autres traitements automatisés de données à caractère personnel, à l'épreuve du nouveau règlement général sur la protection des données », *Bull. Ass.*, 2018/3, pp. 307 et s.

disposition (décision ; fondée exclusivement sur un traitement automatisé ; produisant des effets juridiques ou l'affectant de manière significative) peuvent en effet être satisfaites en cas d'utilisation de l'IA par une compagnie d'assurances pour décider de couvrir un risque donné ou établir une tarification.

L'interdiction ne s'applique toutefois pas si l'une des trois hypothèses de l'article 22, § 2, du RGPD est rencontrée, autrement dit lorsque « la décision :

a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;
b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou
c) est fondée sur le consentement explicite de la personne concernée ».

Des informations spécifiques devront également être communiquées à la personne concernée, en vertu des articles 13 à 15 du RGPD : elles portent sur « l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ».

Comme l'a jugé la Cour de justice, « ces exigences plus élevées quant à la licéité d'une prise de décision automatisée ainsi que les obligations d'information supplémentaires du responsable du traitement et les droits d'accès supplémentaires de la personne concernée qui y sont liés s'expliquent par la finalité que l'article 22 du RGPD poursuit, consistant à protéger les personnes contre les risques particuliers pour leurs droits et libertés que présente le traitement automatisé de données à caractère personnel, y compris le profilage » (154).

On peut s'interroger sur la manière d'articuler cette disposition avec les règles désormais prévues par le règlement IA. L'approche n'étant pas la même, plusieurs différences peuvent être constatées, en fonction de la qualification du système d'IA.

L'article 22 du RGPD concerne uniquement les décisions fondées *exclusivement* sur un traitement automatisé (et donc sans intervention humaine). Dès lors qu'un contrôle humain est effectivement mis en œuvre, cette disposition ne doit pas être observée. Pour les systèmes d'IA à haut risque, l'article 14 du règlement IA exige, en son paragraphe 1er, que « la conception et le développement des systèmes d'IA à

(154) C.J., 7 décembre 2023, aff. C-634/21, *OQ c. Land Hessen, en présence de Schufa Holding AG*, EU:C:2023:957, point 57. Cet arrêt apporte d'autres enseignements utiles à l'interprétation de l'article 22 : il décide ainsi que « l'article 22, paragraphe 1, du RGPD doit être interprété en ce sens que l'établissement automatisé, par une société fournissant des informations commerciales, d'une valeur de probabilité fondée sur des données à caractère personnel relatives à une personne et concernant la capacité de celle-ci à honorer des engagements de paiement à l'avenir constitue une « décision individuelle automatisée », au sens de cette disposition, lorsque dépend de manière déterminante de cette valeur de probabilité le fait qu'une tierce partie, à laquelle ladite valeur de probabilité est communiquée, établisse, exécute ou mette fin à une relation contractuelle avec cette personne » (point 78). Dans le cadre de cette contribution, nous pouvons difficilement procéder à une analyse détaillée. Voy. à ce sujet J. De Cooman et M. Dejaer, « (Il)légalité de la prise de décision automatisée après Schufa (C-634/21) et avant le Règlement (UE) sur l'intelligence artificielle (AI Act) : un pas en avant, deux pas en arrière ? », *R.D.T.I.*, 2024, à paraître.

haut risque permettent, notamment au moyen d'interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant leur période d'utilisation ». Il ajoute, à l'article 26, § 2, que « les déployeurs confient le contrôle humain à des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaire, ainsi que du soutien nécessaire ».

Il est également intéressant de mettre en perspective le droit à l'information des articles 13-15 du RGPD et le droit à l'explication des décisions individuelles prévu à l'article 86 de l'AI Act. Le paragraphe 1er de cette disposition énonce en effet que « toute personne concernée faisant l'objet d'une décision prise par un déployeur sur la base des sorties d'un système d'IA à haut risque mentionné à l'annexe III, à l'exception des systèmes énumérés au point 2 de ladite annexe, et qui produit des effets juridiques ou affecte significativement cette personne de façon similaire d'une manière qu'elle considère comme ayant des conséquences négatives sur sa santé, sa sécurité ou ses droits fondamentaux a le droit d'obtenir du déployeur des explications claires et pertinentes sur le rôle du système d'IA dans la procédure décisionnelle et sur les principaux éléments de la décision prise ». A nouveau, seuls les systèmes d'IA à haut risque sont concernés, plus précisément ceux qui sont référencés à l'annexe III (ce qui exclut les systèmes d'IA qualifiés à haut risque sur le fondement de l'article 6, § 1er). La personne a le droit d'obtenir des « explications claires et pertinentes sur le rôle du système d'IA dans la procédure décisionnelle et sur les principaux éléments de la décision prise », ce qui nous paraît plus contraignant que la seule exigence d'informations utiles sur la logique sous-jacente, dont la portée est discutée.

S'agissant par contre des systèmes d'IA qui présentent un risque spécifique en matière de transparence ou un risque minimal, aucune exigence n'est posée par l'AI Act relativement à l'intervention d'un facteur humain ou à un droit d'explication sur le rôle joué par le système d'IA ou sur les principaux éléments de la décision prise. Les dispositions du RGPD continueront donc à s'appliquer et à offrir une première ligne de protection à la personne concernée.

Conclusions

34. Nouveau cadre réglementaire à respecter par les compagnies d'assurances et les intermédiaires. Les nombreux textes adoptés par le législateur européen au cours des derniers mois dans le domaine du numérique peuvent s'appliquer au secteur des assurances. Lorsque des données à caractère personnel sont traitées (ce qui sera souvent le cas), les dispositions du RGPD devront également être respectées.

Dans la présente contribution, nous avons analysé certains de ces nouveaux textes, de manière générale (pour le DSA et DORA) ou de façon plus détaillée (pour le DA et l'AIA), pour mettre en évidence des lignes de convergence, et des différences éventuelles, avec le RGPD.

Ces textes sont longs et particulièrement complexes, notamment sur le plan technique. Aussi faut-il conseiller aux compagnies d'assurance potentiellement concernées de veiller à leur mise en œuvre dès que possible. Parallèlement (et à l'instar de ce que l'on a connu pour le RGPD), ils ne manqueront pas de poser des questions d'interprétation, que la Cour de justice sera amenée à trancher dans les années à venir.

35. Comment articuler les textes ? Les dispositions du RGPD devront généralement être respectées en même temps que celles prévues par le DSA, DORA, le DA ou l'AIA.

Lorsque les règles sont complémentaires, cela ne posera pas de difficulté majeure. Tel est le cas dans le DSA ou dans DORA, sous réserve de l'intervention des autorités compétentes et des mesures visant à rechercher et prévenir les infractions, pour lesquelles on espère une coopération efficace au stade de la mise en œuvre des règles.

Dans le DA, les nouveaux droits d'accès et à la portabilité des données reconnus à l'utilisateur d'un produit connecté ou d'un service connexe devraient être perçus comme complémentaires aux droits d'accès et à la portabilité des données consacrés par le RGPD dans l'hypothèse où cet utilisateur a la qualité de « personne concernée ». En ce sens, la mise en œuvre de ces droits ne semble *a priori* pas créer de grandes difficultés d'articulation avec le RGPD. Du reste, le DA prévoit que les dispositions du RGPD prévalent en cas de conflit. En pratique, il conviendra donc d'être particulièrement attentif au respect du RGPD lorsque les données qui doivent être mises à disposition de l'utilisateur ou d'un tiers par application du DA sont des données à caractère personnel relatives à une personne autre que l'utilisateur.

S'agissant enfin de l'AIA, qui vise certains aspects de protection des données, une distinction devra être faite en fonction du système d'IA considéré ou du recours à un modèle d'IA à usage général. S'il est à haut risque, des exigences spécifiques devront être observées et, le cas échéant, articulées avec celles du RGPD.