L'Union européenne et la circulation des données

Ledger, Michele; Michaux, Benoit

Published in:
Journal des Tribunaux

Publication date:
2024

Document Version
le PDF de l'éditeur

L'Union européenne et la circulation des données : vers un cadre normatif global ?

1 Introduction : les premières étapes de la réglementation de l'Union sur les données

1. Depuis 2014, les autorités de l'Union européenne multiplient les initiatives destinées à réglementer les données. L'accélération de l'activité législative était devenue inévitable sous la pression des volumes de données générés par les technologies numériques ainsi que des transformations de l'économie et de la société qui en ont résulté.

Durant la période s'étalant entre 2014 et 2020, le développement du cadre normatif s'est révélé particulièrement significatif, tant au regard du nombre de textes adoptés que des ambitions nourries par les autorités. Première pierre à l'édifice : en 2016, c'est l'adoption du « RGPD » consacré au traitement des données à caractère personnel (le Règlement général sur les données personnelles) qui a entre autres pour but de renforcer la confiance dans la société numérique[1]. Le RGPD remplace la directive 95/46[2]. Il l'améliore, entre autres, en renforçant les droits existants et en ajoutant de nouveaux droits au bénéfice des personnes concernées (à savoir : le droit à l'oubli, le droit de ne pas être soumis à un profilage, et le droit à la portabilité des données)[3].

L'Union s'est ensuite dotée de trois instruments complémentaires qui ont étendu le champ d'organisation du marché digital des données, en incluant cette fois les données *non* personnelles. Le premier de ces instruments consiste précisément dans le « règlement relatif à la libre circulation des données à caractère non personnel »[4]. Cette dernière notion vise par exemple les données générées par des objets connectés à Internet (tels que des appareils domestiques) à des fins de maintenance[5]. Pour apprécier les implications de ce règlement, il est utile de se référer aux lignes directrices établies par la Commission. Celles-ci « visent à aider les utilisateurs — en particulier les petites et moyennes entreprises — à comprendre l'interaction entre le règlement relatif au libre flux des données à caractère non personnel et le RGPD. Elles portent donc, plus particulièrement, sur i) les concepts de données à caractère non personnel et de données à caractère personnel, ii) les principes de libre circulation des données et d'interdiction des exigences de localisation des données en vertu des deux règlements, et iii) la notion de portabilité des données dans le cadre du règlement sur le libre flux des données à caractère non personnel. Elles couvrent également les exigences d'autorégulation établies dans les deux règlements »[6].

Le deuxième instrument complémentaire adopté par l'Union correspond au « règlement sur la cybersécurité »[7]. Ce texte a pour objectif général d'accroître la sécurité et la résilience des services en ligne, par l'entremise d'une agence dédiée (« l'Agence européenne pour la cybersécurité ») et de la mise en place d'un cadre pour des schémas de certification[8]. Le règlement vise notamment à écarter toute forme de cybermenace susceptible de porter atteinte aux intérêts des utilisateurs de réseaux et de systèmes d'information — et donc entre autres aux données personnelles de ces derniers, ou à des données non personnelles. En particulier, il impose l'obligation de vérifier la fiabilité des produits et services en cause sur le plan du respect des garanties d'intégrité et de confidentialité des données stockées, et ce dès la conception des produits et services en question. En cas d'évaluation positive, un certificat de conformité sera délivré, qui devra être reconnu dans tous les États membres — y compris, dès lors, dans les États autres que celui dans lequel le certificat a été octroyé. Les normes à respecter pour l'obtention du certificat sont établies sous le contrôle de l'Agence — ce contrôle constituant une de ses tâches essentielles.

Quant au troisième instrument complémentaire que l'Union a mis en place, il s'agit de la directive généralement désignée par l'acronyme « PSI »[9], à savoir « la directive sur les données ouvertes et la réutilisation des informations du secteur public », telle que refondue de manière substantielle en 2019[10]. Il existait déjà auparavant une directive consacrée à « l'open data »[11] qui, en 2013, avait elle-même amélioré la directive initiale que le législateur de l'Union avait consacrée à la réutilisation des informations du secteur public en 2003[12]. Alors qu'au départ, la première directive (2003) se limitait à encourager les organismes du secteur public à autoriser la réutilisation de leurs informations, la deuxième (2013) a instauré une véritable obligation en ce sens et a établi en outre une politique de « données ouvertes ». Il restait cependant du chemin à accomplir ; c'est de cette tâche que s'est acquittée la troisième directive (2019), notamment en imposant des techniques appropriées pour assurer l'ouverture effective des données et en faisant de l'accès obligatoire aux données un accès en temps réel et à des données dynamiques[13].

2. Durant cette même période (2014 à 2020), l'Union a également mis en place des législations sectorielles, car le besoin s'était fait sentir de corriger certaines défaillances du marché par rapport aux données dans des domaines d'activités spécifiques, à savoir, en particulier : l'automobile[14], les services de paiement[15], les compteurs intelli-

(1) Règlement (UE) 2016/679 « 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 ». Pour des articles présentant une introduction générale au règlement, voy. K. Janssens et M. Nuytten, « De Algemene Verordening Persoonsgegevens : van theorie naar praktijk », *R.D.C.-T.B.H.*, 2018/5, pp. 401-435 ; R. Robert et C. Ponsart, « Le règlement européen de protection des données personnelles », *J.T.*, 2018/20, n° 6732, pp. 421-438. Pour un ouvrage donnant un aperçu pratique et plus détaillé, voy. C. De Terwangne, E. Degrave, A. . Delforge et L. Gérard, *La protection des données à caractère personnel en Belgique*, Bruxelles, Politeia, 2019, 190 p.

(2) Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(3) À propos de certains aspects de ce règlement, voy. la contribution publiée dans le prochain numéro du *Journal des tribunaux*.

(4) Règlement (UE) 2018/1807.

(5) On ajoutera à cet exemple, le cas des données anonymisées. Voy. à cet égard, T. Tombal, *Imposing Data Sharing among Private Actors*, Alphen, Kluwer, 2022, p. 22, n° 18.

(6) Communication de la Commission au Parlement et au Conseil, « Lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne », COM (2019) 250, p. 3.

(7) Règlement (UE) 2019/881. Pour un commentaire, voy. P. Valcke, P. S. Royer, et M. Fierens, « Cyberbeveiliging : een blik op het amalgaam van Europese en Belgische regels », *R.W.*, 2020-2021/9, pp. 322-335.

(8) Voy. à ce sujet M. Knockaert, « Chapitre 3 - La sécurité dans le marché unique numérique européen : le Règlement 2019/881 ("Cybersecurity Act") », *in* F. Dumortier *e.a.* (dir.), *Les obligations légales de cybersécurité et de notifications d'incidents*, Bruxelles, Politeia, 2019, pp. 161-183.

(9) Dérivé de la désignation anglaise : « Public Sector Information ».

(10) Directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 (refonte) concernant les données ouvertes et la réutilisation des informations du secteur public. Il en sera question dans la contribution publiée dans le prochain numéro du *Journal des tribunaux*.

(11) Directive (UE) 2013/37 du Parlement européen et du Conseil du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public. Voy. à cet égard M. Knockaert, « La réutilisation des informations du secteur public : l'open data et les organismes publics », *J.T.*, 2018, pp. 613-621. Pour une analyse de la transposition en Belgique de cette directive, voy. F. Schram, « Hergebruik van overheidsinformatie op het federale niveau », *C.D.P.K.*, 2017/1-2, pp. 103-130.

(12) Directive (CE) 2003/98 du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public.

(13) Voy. pour une analyse plus approfondie de cette directive la contribution publiée dans le prochain numéro du *Journal des tribunaux*.

(14) Règlement (CE) n° 715/2007 tel que modifié par le règlement (CE) n° 595/2009.

(15) Directive 2015/2366 relative aux services de paiement.

gents[16], les réseaux d'électricité[17] et les systèmes de transport intelligents[18].

Par ailleurs, à la même époque, l'Union a également adopté une législation destinée à protéger les consommateurs qui accordent un accès à leurs données aux fournisseurs de services numériques[19].

3. Certes, le bond législatif réalisé entre 2014 et 2020 ne doit pas faire oublier les prémices qui étaient intervenues dès le milieu des années 1990. À cet égard, on signalera, outre la directive 95/46 (« relative au traitement des données à caractère personnel ») et la directive 2003/98 (« relative à la réutilisation des informations du secteur public ») — toutes deux déjà mentionnées, la directive 96/9[20], destinée à récompenser les investissements des producteurs de bases de données[21]. Il faut toutefois concéder rétrospectivement que ces prémices de la première période (1995-2013) s'avèrent plutôt modestes quand on les compare aux développements que nous venons d'évoquer à propos de la deuxième période (2014-2020) — ces derniers méritant, eux, d'être qualifiés de considérables.

4. Cela étant, quelque remarquable que soit l'importance du travail législatif fourni durant la deuxième période, il est apparu que des progrès essentiels devaient encore être accomplis pour optimaliser et préciser la réglementation des données à l'échelle de l'Union. Surtout, avant d'aller plus loin dans ce domaine, il est apparu aux autorités qu'il s'imposait au préalable de définir une stratégie globale en matière de données et de se doter, à cette fin, d'un document fondateur susceptible de proposer une politique à long terme : ce sera l'objet du document adopté par la Commission en février 2020, intitulé « Communication pour une stratégie européenne des données »[22].

2 Un document stratégique et trois nouveaux règlements

5. Dans la communication de février 2020, l'objectif ultime des autorités de l'Union s'affiche comme suit : l'Union européenne (UE) a pour ambition de « devenir un modèle de premier plan pour une société à laquelle les données confèrent les moyens de prendre de meilleures décisions, tant pour les entreprises que dans le secteur public »[23].

Pour que l'Union européenne puisse jouer ce rôle moteur, la Commission prépare tout à la fois l'harmonisation nécessaire, notamment des questions de connectivité, de traitement et de stockage, mais également l'amélioration des structures de gouvernance et l'augmentation des réserves communes de données afin de permettre leur (ré)utilisation.

L'ampleur de ce déploiement d'actions multiples se justifie au regard des enjeux économiques et sociétaux qui revêtent une envergure de premier ordre[24]. Sur le plan économique, les données sont vitales et constituent la base de nombreux nouveaux services et produits dans tous les secteurs, y compris pour les start-ups et les PME. Sur le plan sociétal, augmenter la masse de données disponibles tout en améliorant leurs conditions d'utilisation équivaut à accroître la perspective de pouvoir relever les défis sociétaux, climatiques et environnementaux et de contribuer ainsi à une société plus saine, plus prospère et plus durable.

La tâche s'annonce toutefois ardue puisque « une grande partie des données du monde entier sont aux mains d'un petit nombre d'entreprises de haute technologie »[25]. De plus, il faut tirer la leçon des pratiques observées chez les concurrents de l'Union : « Aux États-Unis, l'organisation de données est laissée au secteur privé, avec des effets de concentration considérables. La Chine combine une surveillance gouvernementale avec un fort contrôle des grandes entreprises de haute technologie sur des volumes massifs de données sans garanties suffisantes pour les particuliers »[26]. La Commission se donne donc pour mission de trouver sa « propre voie européenne, en équilibrant le flux et la large utilisation des données, tout en préservant des normes élevées en matière de vie privée[27], de sécurité, de sûreté et d'éthique »[28].

Le but de l'Union est dès lors de créer un espace européen unique pour les données qui devrait garantir que celles-ci puissent circuler au sein des vingt-sept États membres. Il importe en effet de mettre rapidement un terme à la fragmentation de l'arsenal législatif au sein de l'Union — certains États membres (parmi lesquels la France et la Finlande) ayant par exemple commencé à légiférer sur l'utilisation par les pouvoirs publics de données détenues par le secteur privé.

6. La présente contribution vise à décrire les trois initiatives majeures intervenues depuis la publication de cette Communication, à savoir le « règlement portant sur la gouvernance européenne des données » (« Data Governance Act », en abrégé « DGA »)[29], le « règlement relatif aux marchés contestables et équitables dans le secteur numérique » (le « Digital Markets Act », en abrégé « DMA »)[30] et enfin le « règlement concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données » aussi appelé le « règlement sur les données » (en abrégé « Data Act » ou « DA »)[31].

Nous ne traitons donc pas ici dans le détail des textes suivants, déjà évoqués plus haut et dont certains seront pour partie discutés ailleurs dans le prochain numéro du *Journal des tribunaux* : le « règlement général sur la protection des données » (« RGPD »)[32], le « règlement relatif à la libre circulation des données à caractère non personnel dans l'UE »[33], le « règlement sur la cybersécurité »[34], et la « directive sur les données ouvertes »[35].

Nous n'examinons pas non plus ici le « règlement relatif à un marché unique des services numériques » (« Digital Services Act », en abrégé « DSA »)[36], dès lors que celui-ci ne cherche pas à assurer une circula-

(16) Directive 2019/944 pour l'électricité et directive 2009/73/CE pour les compteurs de gaz.
(17) Règlement (UE) 2017/1485 de la Commission et règlement (UE) 2015/703 de la Commission.
(18) Directive 2010/40/UE.
(19) Directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques.
(20) Directive 96/9 concernant la protection juridique des bases de données. Pour un aperçu général de la protection, voy. H. VANHEES, « Hoofdstuk 4 - De bescherming van databanken », *in Handboek intellectuele rechten*, Bruxelles, Intersentia, 2020, pp. 193-230.
(21) Pour un regard critique sur l'évolution de la protection accordée par cette directive, voy. notamment E. DERCLAYE et M. HUSOVEC, « La Cour de justice amincit le droit *sui generis* sur les bases de données - L'affaire *CV-Online Latvia c. Melons* souligne l'importance de l'accès à l'information et de la concurrence dans l'appréciation de la contrefaçon du droit sui generis », *A&M*, 2021/4, pp. 458-461.
(22) Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions « Une stratégie européenne pour les données », 19 février 2020, COM/2020/66 final.
(23) Communication « Une stratégie européenne pour les données », note 22 *supra*, p. 1.
(24) Voy. le regard d'ensemble que Tombal a porté sur cette thématique : T. TOMBAL, *Imposing data sharing among private actors : a tale of evolving balances*, *op. cit.*, 463 p.
(25) Communication « Une stratégie européenne pour les données », p. 3.
(26) Communication « Une stratégie européenne pour les données », p. 4.
(27) On fera le lien ici avec le RGPD (2016/679) qui consacre le *corpus* des règles de protection des données à considérer comme un pilier de la politique européenne en matière de données (*cfr* note 1 *supra*).
(28) Communication « Une stratégie européenne pour les données », p. 4.
(29) Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), *J.O.* L 152 du 3 juin 2022, pp. 1-44. Ce règlement (« DGA ») prévoit une entrée en vigueur le 23 juin 2022, et une mise en application à partir du 24 septembre 2023.
(30) Règlement (UE) 2022/1925 du Parlement européen et du Conseil 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 du 12. octobre2022, pp. 1-66. Ce règlement (« DMA ») prévoit une entrée en vigueur le 1er novembre 2022, et une mise en application à partir du 2 mai 2023.
(31) 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, pp. 1-71. Ce règlement (« DA ») prévoit une entrée en vigueur le 11 janvier 2024, et une mise en application à partir du 12 septembre 2025.
(32) Règlement (UE) 2016/679.
(33) Règlement (UE) 2018/1807.
(34) Règlement (UE) 2019/881.
(35) Directive (UE) 2019/1024.
(36) Règlement (UE) 2022/2065 du Parlement et du Conseil, du 19 octobre 2022, relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE

tion des données — en vue de leur (ré-)exploitation. Il importe toutefois de mentionner les axes principaux de cet instrument, même s'il tombe en dehors du champ de notre étude, ne fût-ce que pour le situer dans le nouveau paysage législatif européen (celui qui fait suite à la communication de février 2020). Parmi ses objectifs majeurs, le DSA vise à compléter et à préciser les obligations des fournisseurs de services en ligne, en particulier les plateformes, quand il s'agit d'agir contre des contenus illicites, d'assurer la transparence de la publicité (notamment concernant l'identité de l'annonceur), de protéger les mineurs. Le DSA prévoit en outre des obligations spécifiques à charge des « fournisseurs de très grandes plateformes et de très grands moteurs de recherche » ; si, dans ce cadre-ci, il organise un accès à des données, il s'agit d'un accès dont le but se limite à permettre aux instances compétentes de surveiller le respect du règlement par les plateformes et moteurs de recherche en cause[37] : les données ne sont pas destinées à être (ré-)exploitées.

7. Les trois initiatives commentées ici présentent un certain nombre de points communs.

Tout d'abord, il s'agit de règlements et non de directives, ce qui signifie qu'il s'agit de textes directement applicables en droit national. En outre, ils concernent tous les trois l'accès et la (ré)-utilisation des données au sens large — la notion de donnée étant définie dans les trois textes comme étant « 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 ». Ces textes ne font donc pas de distinction entre les données personnelles et non personnelles, ce qui n'empêche pas que les données à caractère personnel resteront par ailleurs soumises au régime du RGPD pour ce qui est de leur traitement. Enfin, les trois initiatives assignent un rôle important à des autorités de contrôle qui devront être mises en place par les États membres.

En marge de ce qui précède, précisons qu'au moment où nous rédigeons la présente contribution les règlements DGA et DMA sont tous deux applicables depuis peu[38], alors que le Data Act, quant à lui, ne l'est pas encore[39].

3 Data Governance Act (règlement (UE) 2022/868)

8. Le « règlement portant sur la gouvernance européenne des données » (« le DGA »)[40] est la première pièce de l'édifice réglementaire envisagé dans la stratégie de la Commission — telle que présentée dans la Communication du 19 février 2020[41]. Il est d'application depuis le 24 septembre 2023 dans les États membres.

Le DGA comporte principalement trois nouveautés. Il complète d'abord la directive dite PSI sur les données ouvertes[42] en créant un mécanisme particulier pour la réutilisation de certaines catégories spécifiques de données détenues par des organismes du secteur public (ces catégories ayant été elles-mêmes exclues de la directive précitée) : il s'agit des données sujettes à des droits des tiers (par exemple des données protégées par des droits de propriété intellectuelle). De plus, ce règlement établit un cadre pour la notification et le contrôle de services d'intermédiation de données. Enfin, il met sur pied un système normatif pour l'utilisation et le partage de données pour des raisons dites « altruistes ».

9. La première innovation principale du DGA concerne les conditions de réutilisation des données détenues par les organismes du secteur public. Le règlement instaure des règles particulières pour certaines catégories spécifiques de données, à savoir celles qui sont protégées pour des motifs de confidentialité commerciale (en ce compris le secret d'affaires), de secret statistique, de protection de la propriété intellectuelle de tiers ou de protection des données à caractère personnel[43]. Afin de favoriser l'utilisation de ces données, le règlement prévoit quatre règles.

En premier lieu, les organismes du secteur public se voient interdire principalement la conclusion d'accords qui pourraient avoir pour objet ou effet d'octroyer des droits d'exclusivité pour la réutilisation des données en cause. Néanmoins, un droit d'exclusivité peut être accordé dans la mesure nécessaire à la fourniture d'un service ou d'un produit d'intérêt général qui, sans cela, ne pourrait pas être obtenu ; dans ce dernier cas, la durée du droit d'exclusivité pour la réutilisation des données ne pourra toutefois pas dépasser douze mois[44].

En second lieu, ces organismes doivent rendre publiques les conditions de réutilisation des données et la procédure de demande via un point d'information unique[45]. Les conditions de réutilisation doivent être non discriminatoires, transparentes, proportionnées et objectivement justifiées[46] et elles doivent veiller à préserver le caractère protégé des données[47] en prévoyant par exemple qu'elles ont été anonymisées (pour les données personnelles) ou que l'accès aux données et leur utilisation se déroulent dans un environnement sécurisé sous le contrôle de l'organisme public[48]. Lorsqu'il est impossible d'autoriser la réutilisation des données, l'organisme public doit tout mettre en œuvre pour aider les re-utilisateurs potentiels à demander le consentement des personnes concernées (ou des détenteurs de droits intellectuels sur les données) si ceci n'engendre pas des coûts disproportionnés pour l'organisme public[49]. La réutilisation des données ne pourra se faire que dans le respect a) des droits de propriété intellectuelle, sachant que les organismes publics ne peuvent pas exercer le droit du fabricant d'une base de données[50] et b) de la confidentialité des données qui ne pourront pas être divulguées du fait de l'autorisation[51].

En troisième lieu, les organismes publics peuvent percevoir des redevances[52] pour autoriser la réutilisation des données.

En quatrième lieu, les organismes publics doivent adopter une décision sur la demande de réutilisation des données dans un délai de deux mois à compter de la réception de la demande, sauf si des délais plus courts sont fixés par le droit national[53]. Par ailleurs, les États membres doivent désigner un ou plusieurs organismes compétents afin d'assister les organismes publics lorsqu'ils octroient ou refusent l'accès aux données à des fins de réutilisation[54]. Ces organismes compétents pourront aussi être habilités à octroyer eux-mêmes l'accès aux données. Ils doivent disposer de ressources[55] suffisantes pour mener à bien leurs tâches d'assistance qui sont également énumérées dans le règlement à titre exemplatif : une assistance technique (telle que la mise à disposition d'un environnement de traitement sécurisé ou la fourniture d'orientations sur la meilleure manière de structurer et de stocker les données pour les rendre facilement accessibles) ou une assistance en vue d'obtenir le consentement des personnes concernées[56].

10. La deuxième innovation du DGA vise à favoriser un environnement compétitif et la confiance que le législateur européen a estimés nécessaires pour le partage des données. À cette fin, le DGA crée un cadre réglementaire à l'échelle de l'Union pour permettre l'émergence de services d'intermédiation de données[57] neutres[58] et fiables. Ces in-

(« règlement sur les services numériques », ci-après « Digital Services Act » ou « DSA »).
(37) Article 40 du DSA. Voy. aussi *infra*, n° 14.
(38) Voy. *supra*, notes 29 et 30. Le DGA est entré en vigueur le 23 juin 2022 et il est applicable à partir du 24 septembre 2023. Le DMA est entré en vigueur le 1er novembre 2022 et il est applicable depuis le 2 mai 2023.
(39) Voy. *supra*, note 31. Le DA entre en vigueur le 11 janvier 2024 et il sera applicable à partir du 12 septembre 2025.
(40) Voy. les références complètes du règlement à la note 29.
(41) Communication « Une stratégie européenne pour les données » : voy. *supra*, note 22.
(42) Voy. *supra*, notes 9-11.
(43) Article 3.1 du DGA.
(44) Article 4 du DGA.
(45) Article 5.1 du DGA.
(46) Article 5.2 du DGA.
(47) Article 5.3 du DGA.
(48) Article 5.3 du DGA.
(49) Article 5.6 du DGA.
(50) Article 5.7 du DGA.
(51) Article 5.8 du DGA.
(52) Pour autant que les redevances soient transparentes, non discriminatoires, proportionnées et objectivement justifiées et qu'elles ne restreignent pas la concurrence (article 6 du DGA).
(53) Article 9 du DGA.
(54) Article 7.1 du DGA.
(55) L'article 7.3 du DGA prévoit qu'il s'agit de ressources juridiques, financières, techniques et humaines.
(56) Article 7.4 du DGA.
(57) Un service d'intermédiation est défini comme un service qui vise à établir des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et d'utilisateurs de données, d'autre part, par des moyens techniques, juridiques ou autres, y compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel, à l'exclusion au minimum de ce qui suit : a) des services qui obtiennent des données auprès des détenteurs de données et les agrègent, les enrichissent ou les

termédiaires sont appelés à faciliter l'échange de données, par le biais de services tels que le stockage, l'organisation, la conversion ou l'anonymisation des données[59]. Aux termes du DGA, le prestataire de services d'intermédiation de données doit 1) notifier son intention de fournir un tel service à l'autorité compétente de l'État membre de son établissement principal[60], en fournissant les renseignements requis, 2) apposer un logo commun d'identification (conçu par la Commission européenne) sur chaque publication qui se rapporte à ses activités d'intermédiation de données[61] et 3) se soumettre à des conditions liées à la fourniture de services d'intermédiation de données (quinze exigences sont prévues qui visent à assurer la neutralité des prestataires ; il s'agit d'exigences qui concernent la sécurité des données et des systèmes utilisés, l'interopérabilité et le partage des données, l'accès équitable et non discriminatoire au service d'intermédiation, et des mesures en cas d'insolvabilité des prestataires)[62].

Le DGA prévoit également que chaque État membre désigne une ou plusieurs autorités compétentes pour effectuer les tâches liées à la procédure de notification (en ce compris la transmission à la Commission européenne de la liste des services notifiés, en vue d'établir un registre public de tous les services d'intermédiation de données qui proposent leurs services au sein de l'Union)[63] et de contrôler le respect des dispositions. Ces autorités compétentes ont le pouvoir d'imposer par le biais de procédures administratives des sanctions financières, y compris des astreintes, d'engager des procédures judiciaires ou même d'exiger la cessation de l'activité[64]. On observera au passage que ce nouveau cadre réglementaire, dont les effets sont particulièrement sévères même si les visées sont louables, n'a pas manqué de susciter des premières réflexions critiques au nom du principe de libre entreprise[65].

11. La troisième innovation principale du DGA porte sur l'introduction d'un cadre normatif destiné à faciliter le partage de données à titre « altruiste ».

Le texte part de l'idée que certaines personnes pourraient être prêtes à mettre leurs données à disposition sur une base volontaire pour des buts d'intérêt général, la seule compensation qu'elles revendiqueraient étant limitée aux coûts qu'elles supporteraient pour cette mise à disposition[66]. Il s'agit de ce qui est appelé « altruisme en matière de données », dont le DGA entend favoriser le développement. S'il est difficile à ce stade d'identifier avec précision les cas pratiques susceptibles de se présenter à l'avenir (tout pronostic serait aléatoire), on peut néanmoins esquisser quelques possibilités à partir des objectifs d'intérêt général mentionnés à titre d'exemples dans le DGA. Ainsi pourrait-on songer en particulier au domaine de la mobilité où des données de géolocalisation pourraient être partagées par des opérateurs au moyen d'un *data pool* au départ duquel les données, une fois centralisées, seraient partagées pour favoriser une mobilité intégrée entre des transports en commun, améliorer un service de vélos partagés, ou encore réduire les temps d'attente aux bornes de recharge.

Au sein de ce système, les organisations dites altruistes se voient assigner un rôle essentiel. Si leur fonctionnement ne ressort pas du texte avec toute la limpidité voulue, on peut néanmoins proposer ici un aperçu articulé de la manière dont le DGA semble concevoir les rouages de cette mécanique. Il apparaît ainsi que les organisations altruistes reçoivent une mission d'intermédiaire de confiance pour gérer dans les règles les données que les personnes concernées[67] mettent à la disposition de la communauté dans le but de servir un objectif d'intérêt général. D'une part, les organisations altruistes doivent fournir aux personnes concernées les informations pertinentes concernant les objectifs d'intérêt général qui seront poursuivis ainsi que le traitement réservé aux données[68]. D'autre part, elles doivent rendre compte auprès des autorités de la manière dont les objectifs d'intérêt général sont promus et de l'identité des personnes qu'elles ont autorisées à traiter les données ainsi que des modalités de traitement des données[69].

Pour mettre en évidence le crédit qui leur est dû, le DGA prévoit que les organisations sont admises à utiliser le label « organisation altruiste en matière de données reconnue dans l'Union »[70]. Elles doivent cependant veiller à être enregistrées au préalable (après en avoir obtenu l'autorisation) dans le registre public national par l'autorité nationale compétente dont elles relèvent[71], chaque État membre ayant l'obligation de désigner une ou plusieurs autorités compétentes à cet effet[72]. Parmi les conditions à remplir pour obtenir l'enregistrement dans le registre public national, l'organisation concernée doit être une personne morale constituée en vertu du droit national pour poursuivre des objectifs d'intérêt général[73]. L'organisation altruiste se voit imposer des exigences supplémentaires, notamment celle de ne pas utiliser les données pour d'autres objectifs que ceux d'intérêt général autorisés, celle de permettre aux personnes concernées de retirer leur consentement et celle d'assurer la sécurité des données[74]. Les autorités nationales désignées par les États membres ont la mission de contrôler les organisations pour s'assurer que celles-ci respectent les exigences qui pèsent sur elles[75].

12. Pour terminer, on signalera que le DGA — à l'instar de la plupart des textes européens plus récents — comprend un chapitre approfondi consacré aux différentes autorités compétentes chargées du contrôle, ainsi qu'aux dispositions procédurales.

S'agissant des autorités compétentes, on relèvera au passage que le règlement risque de créer des situations complexes : la liberté laissée aux États membres peut avoir pour effet que dans un même État, plusieurs autorités soient compétentes pour superviser le respect du même règlement[76], et que des divergences de choix surgissent d'un État à l'autre. Quant à leurs activités, le DGA prévoit que les autorités compétentes en matière de services d'intermédiation des données et pour l'enregistrement des organisations altruistes doivent être indépendantes, disposer des ressources humaines et financières suffisantes et accomplir leurs tâches de façon impartiale, transparente, cohérente, fiable et rapide[77]. Toute personne physique ou morale lésée a le droit d'introduire une réclamation auprès de l'autorité compétente qui devra informer l'auteur de la réclamation de l'état d'avancement de la procédure et de la décision prise, ainsi que des recours juridictionnels dont les personnes devront également toujours disposer[78].

Par ailleurs, le règlement prévoit également la création d'un Comité européen de l'innovation dans le domaine des données, sous la forme d'un groupe d'experts et composé des représentants des autorités compétentes nationales et d'autres organes européens tel que le Comité européen de la protection des données[79]. Les missions principales de ce comité sont de conseiller et d'assister la Commission européenne pour les tâches suivantes : (i) l'élaboration d'une pratique cohérente des organismes du secteur public s'agissant de la gestion des de-

transforment afin d'en accroître substantiellement la valeur et concèdent une licence d'utilisation des données résultantes aux utilisateurs de données, sans établir de relation commerciale directe entre les détenteurs de données et les utilisateurs de données ; b) des services axés sur l'intermédiation de contenus protégés par le droit d'auteur ; c) des services utilisés exclusivement par un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient, ou qui sont utilisés par des personnes morales multiples au sein d'un groupe fermé, y compris dans le cadre de relations de fournisseur ou de client ou de collaborations établies par contrat, en particulier ceux qui ont pour principal objectif de garantir les fonctionnalités d'objets et de dispositifs connectés à l'internet des objets ; d) des services pour le partage de données proposés par des organismes du secteur public qui ne cherchent pas à établir des relations commerciales (article 2.11 du DGA).

(58) L'obligation de neutralité implique notamment que l'intermédiaire ne peut pas utiliser lui-même les données : son rôle est de permettre à des tiers d'en faire usage.

(59) Voy. l'article 10 et le considérant 27 du DGA.

(60) Article 11.1 du DGA. Sur base de cette notification, il pourra fournir ses services d'intermédiation dans tous les États membres : article 11.5 du DGA.

(61) Article 11.9 du DGA.

(62) Article 12 du DGA.

(63) Article 13 du DGA.

(64) Article 14 du DGA.

(65) Pour une évaluation critique du nouveau régime, voy. G. Carovano et M. Finck, « Regulating Data Intermediaries : The Impact of the Data Governance Act on the EU's Data Economy (April 18, 2023) ». Accessible en ligne à l'adresse https://ssrn.com/abstract=4422263 ou http://dx.doi.org/10.2139/ssrn.4422263.

(66) Voy. l'article 16 et le considérant 45 du DGA.

(67) L'expression « personnes concernées » désigne ici à la fois les personnes concernées par les données de type personnel et les personnes détentrices des données non personnelles.

(68) Article 21.1 du DGA.

(69) Article 20.2 du DGA. Le règlement impose aux organisations altruistes des obligations liées à la tenue d'un registre public et à la remise de rapports annuels détaillés.

(70) Article 17.2 du DGA.

(71) Article 17.1 du DGA.

(72) Article 23 du DGA.

(73) Article 18 du DGA.

(74) Article 21 du DGA.

(75) Article 24 du DGA.

(76) L'État membre a la faculté de désigner une nouvelle autorité ou une autorité existante (celle-ci pouvant correspondre, par exemple, à l'autorité de protection des données ou l'autorité de protection des consommateurs), voire plusieurs autorités nouvelles ou existantes.

(77) Article 26 du DGA.

(78) Articles 27 et 28 du DGA.

(79) Article 29 du DGA.

mandes de réutilisation des données, (ii) l'élaboration d'une pratique cohérente concernant l'altruisme en matière de données, (iii) l'élaboration d'une pratique cohérente des autorités compétentes s'agissant d'appliquer les exigences auxquelles sont soumis les prestataires de services d'intermédiation des données et (iv) l'élaboration de lignes directrices cohérentes relatives aux exigences en matière de cybersécurité pour l'échange et le stockage des données[80].

Enfin, le règlement traite également la question de l'intervention des juridictions nationales. Dès lors qu'il instaure des pouvoirs décisionnels en faveur d'autorités compétentes[81], il s'attache à déterminer les possibilités de recours contre les décisions prises par ces autorités. Il prévoit à cet égard qu'indépendamment d'un possible recours administratif ou tout autre recours non juridictionnel, la personne lésée par la décision a droit à un recours effectif[82] devant les juridictions de l'État membre de l'autorité en cause[83].

4 Digital Markets Act (règlement (UE) 2022/1925)

13. Le « règlement relatif aux marchés contestables et équitables dans le secteur numérique » (le « Digital Markets Act », « DMA »)[84] a pour objectif d'introduire des règles uniques dans tous les États membres dans le but de prévenir certains abus susceptibles d'être commis par les géants de l'internet[85]. Les opérateurs visés par ce texte y portent le nom de « contrôleurs d'accès de l'internet » (en anglais « gatekeepers » ou gardes-barrières), appellation ainsi réservée aux fournisseurs de services de plateformes dits « essentiels ». En septembre 2023, les contrôleurs d'accès ont été individuellement désignés comme tels par la Commission européenne[86]. Il s'agit des opérateurs suivants : Alphabet, Amazon, Apple, ByteDance, Meta et Microsoft.

14. Les règles instaurées par le DMA sont de nature préventive, par opposition aux règles attachées au droit de la concurrence qui, elles, sanctionnent *a posteriori* les ententes et les abus de position dominante. C'est précisément en raison du fait que le mécanisme *a posteriori* se révèle insuffisant pour contrôler le marché du numérique, que le DMA introduit un système préventif, lequel complète ainsi le droit de la concurrence.

Cela étant, les deux types de législation se rejoignent sur les finalités générales. Le DMA a également pour objectif de lutter contre les pratiques anticoncurrentielles des acteurs dominants et de corriger les déséquilibres liés à leur domination afin de garantir à toutes les entreprises ce que le législateur de l'Union appelle la « contestabilité et l'équité des marchés » dans le secteur du numérique[87]. Dans ce but, le règlement introduit des règles de marché pour ces entreprises sous la forme d'obligations et d'interdictions. Parmi les obligations (dont beaucoup ont été inspirées par des décisions d'autorités de concurrence), figurent des règles d'accès aux données détenues par les opérateurs concernés — c'est-à-dire les contrôleurs d'accès. Les données jouent en effet un rôle clé dans l'économie des plateformes. Ainsi, une des fonctions importantes des plateformes dites « multifaces »[88] est de fournir à ses utilisateurs-vendeurs des données relatives au profil de consommateurs potentiellement intéressants (par exemple un vendeur sur une place de marché qui voudra cibler un potentiel acheteur en fonction de ses achats précédents ou de ses recherches de produits). La plateforme dispose à cet égard des moyens nécessaires pour collecter et analyser les données des utilisateurs-consommateurs en les associant à des algorithmes dans le but de leur offrir des services personnalisés, soit en direct soit via les utilisateurs-vendeurs[89].

Comme cela a déjà été évoqué, le DMA a été proposé en même temps qu'un autre règlement au sein du paquet législatif sur les services numériques, à savoir le DSA[90]. Ce dernier vise avant tout un autre objectif que le DMA : celui de réduire les contenus illégaux et dommageables sur les plateformes tout en respectant les droits fondamentaux (en particulier la liberté d'expression). Dans ce contexte, le DSA instaure des règles d'accès aux données des grandes plateformes et moteurs de recherche. Celles-ci ont pour objectif d'assurer que les instances de contrôle et les chercheurs accrédités puissent évaluer si les plateformes se conforment aux règles du DSA. Elles n'ont donc pas pour objet de faciliter la (ré-)exploitation des données, raison pour laquelle elles sortent du cadre de la présente étude.

15. La notion de contrôleur d'accès est évidemment centrale dès lors que c'est elle qui déclenche l'application du DMA à son égard. Pour la définir, le DMA recourt à trois éléments qui doivent être réunis : l'entreprise en cause a un poids important sur le marché intérieur, elle fournit un service de plateforme essentiel qui constitue un point d'accès majeur permettant aux entreprises utilisatrices d'atteindre leurs utilisateurs finaux et elle jouit d'une position solide et durable dans ses activités, ou jouira, selon toute probabilité, d'une telle position dans un avenir proche[91].

S'agissant du caractère essentiel du service, le DMA le définit par l'énumération de dix catégories de « services de plateforme »[92]. Il s'agit des services d'intermédiation comme les places de marché (Amazon Store, Booking, AliExpress) ou les boutiques d'applications (AppStore, Google Play)[93], ainsi que des moteurs de recherche (Google search, Bing)[94], des réseaux sociaux (Facebook, Instagram, Twitter)[95], des plateformes de partage de vidéos (YouTube)[96], des services de communications interpersonnelles non fondés sur la numérotation comme les messageries en ligne (WhatsApp)[97], des systèmes d'exploitation (macOS, Windows)[98], des navigateurs internet (Internet Explorer, Google Chrome)[99], des assistants virtuels (Alexa)[100], des services en nuage — *cloud* (Microsoft Azure, Amazon AWS)[101] et des services de publicité en ligne[102] fournis par une des entreprises précitées. La Commission peut mener une enquête de marché afin d'examiner s'il conviendrait d'inscrire d'autres services numériques sur la liste et dans

(80) Article 30 du DGA.
(81) Ainsi, l'autorité compétente peut prendre des décisions à l'encontre d'un fournisseur de services d'intermédiation qui manquerait à ses obligations, y compris en lui enjoignant de mettre fin à ses activités d'intermédiation (voy. l'article 14 du DGA).
(82) Article 28.1 du DGA.
(83) Article 28.2 du DGA.
(84) Voy. les références complètes du règlement à la note 30.
(85) Pour une analyse comparative des systèmes de l'UE, du Royaume-Uni, et des États-Unis sur l'approche *ex-ante* de la régulation des plateformes, voy. T. Tombal, « Ensuring contestability and fairness in digital markets through regulation : a comparative analysis of the EU, UK and US approaches », *European Competition Journal*, 2022, 18 :3, 468-500, DOI : 10.1080/17441056.2022.2034331.
(86) Comme prévu, la désignation officielle est intervenue le 6 septembre 2023. Voy. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328.
(87) La « contestabilité » se réfère au caractère critiquable des services de la plateforme en tant que ceux-ci nuisent à l'équité de la relation commerciale entre l'opérateur et les utilisateurs. Voy. à ce propos, notamment, le considérant 2 du DMA.
(88) À titre d'exemple, Amazon peut être considérée comme une plateforme « multiface » : d'une part, elle met en relation des consommateurs et des vendeurs indépendants ; et d'autre part, elle procède elle-même à des ventes directes aux consommateurs.
(89) Voy. à ce sujet M. Bacache-Beauvallet et M. Bourreau, *Économie des plateformes*, Paris, Éditions La Découverte, juin 2022.
(90) Voy. *supra*, n° 6, ainsi que les notes 36 et 37.
(91) Article 3.1 du DMA.
(92) Article 2.2 du DMA.
(93) Au sens de l'article 2. 2 du règlement (UE) 2019/1150 du Parlement et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne.
(94) Au sens de l'article 2. 5 du règlement (UE) 2019/1150.
(95) Défini comme une plateforme permettant aux utilisateurs finaux de se connecter ainsi que de communiquer entre eux, de partager des contenus et de découvrir d'autres utilisateurs et d'autres contenus, sur plusieurs appareils et, en particulier, au moyen de conversations en ligne (chats), de publications (posts), de vidéos et de recommandations.
(96) Au sens de l'article 1er, paragraphe 1, point *abis*), de la directive 2010/13/UE.
(97) Au sens de l'article 2, point 7), de la directive (UE) 2018/1972.
(98) Défini comme un logiciel système qui contrôle les fonctions de base du matériel informatique ou du logiciel et permet d'y faire fonctionner des applications logicielles.
(99) Défini comme une application logicielle qui permet aux utilisateurs finaux d'accéder à des contenus internet hébergés sur des serveurs connectés à des réseaux tels que l'internet, y compris les navigateurs internet autonomes, ainsi que les navigateurs internet intégrés ou inclus dans un logiciel ou équivalent, et d'interagir avec ces contenus.
(100) Défini comme un logiciel qui peut traiter des demandes, des tâches ou des questions, notamment celles fondées sur des données d'entrée sonores, visuelles ou écrites, de gestes ou de mouvements, et qui, sur la base de ces demandes, tâches ou questions, donne accès à d'autres services ou contrôle des appareils connectés physiques.
(101) Au sens de l'article 4, point 19), de la directive (UE) 2016/1148.
(102) Article 2, alinéa 2, sous j), du DMA.

l'affirmative, la Commission devrait proposer une modification législative au DMA[103].

Pour faciliter la mise en application pratique du règlement, le DMA instaure une présomption selon laquelle l'entreprise est réputée répondre aux trois éléments définitionnels du contrôleur d'accès si elle atteint certains seuils quantitatifs en termes de chiffre d'affaires ou de valorisation boursière[104] et de nombre d'utilisateurs[105].

Ainsi, la première condition sera présumée remplie si l'entreprise a réalisé un chiffre d'affaires annuel dans l'UE supérieur ou égal à 7,5 milliards d'euros au cours de chacun des trois derniers exercices, ou si sa capitalisation boursière moyenne (ou sa juste valeur marchande équivalente) a atteint au moins 75 milliards d'euros au cours du dernier exercice, et qu'elle fournit le même service de plateforme essentiel dans au moins trois États membres.

Toute entreprise estimant avoir atteint les seuils requis pour entraîner l'application de la présomption pour un ou plusieurs services de plateforme essentiels doit en informer la Commission par une notification, et cette dernière disposera de quarante-cinq jours ouvrables pour se prononcer sur la question et éventuellement désigner l'entreprise en cause comme étant un contrôleur d'accès pour un ou plusieurs services de plateforme essentiels[106]. L'entreprise peut toutefois contester son statut présumé de contrôleur d'accès[107]. Par ailleurs, même si les seuils ne sont pas atteints, ou si une entreprise conteste son statut présumé, la Commission peut lancer une étude de marché pour examiner si une entreprise doit *in fine* être désignée comme contrôleur d'accès[108]. La Commission devra publier dans le *Journal officiel* de l'UE la liste des contrôleurs d'accès désignés, leurs services essentiels et les obligations auxquelles ils sont soumis[109].

16. Ces entreprises ainsi désignées auront six mois pour se conformer aux vingt-deux obligations énumérées dans le DMA[110]. Certaines de ces obligations et en particulier la plupart de celles relatives à l'accès aux données pourront être « précisées » par la Commission européenne[111] soit de sa propre initiative soit à la demande de l'entreprise concernée[112]. Les autres obligations s'appliquent telles quelles[113].

Autre caractéristique de cette liste d'obligations : certaines s'appliquent à tous les services essentiels (obligations horizontales), tandis que d'autres ne s'appliquent qu'à certaines catégories de services. La plupart des obligations qui concernent les données, sont des obligations horizontales[114].

Parmi les obligations à charge du contrôleur d'accès, celles qui portent sur l'accès aux données, revêtent une importance éminente dès lors que les données constituent un enjeu stratégique du marché numérique unique et qu'elles sont en outre exposées à des risques importants : il est connu que les données sont accaparées en volumes considérables par un nombre limité d'opérateurs dominants, ce qui permet à ceux-ci d'accumuler des connaissances privilégiées et d'acquérir des avantages considérables. Comme le souligne la Commission européenne à ce propos dans sa communication relative à une Stratégie européenne pour les données, « le pouvoir de marché élevé qui résulte de « (l')avantage lié aux données » peut permettre aux grands acteurs de fixer les règles sur la plateforme et d'imposer unilatéralement des conditions d'accès et d'utilisation des données, voire d'utiliser ce pouvoir lorsqu'ils développent de nouveaux services et partent à la conquête de nouveaux marchés »[115].

Les obligations relatives aux données et qui s'imposent à tous les contrôleurs d'accès, sont les suivantes :

— Assurer que les utilisateurs finaux (et les tiers autorisés par eux) puissent 'porter' les données fournies par eux ou générées par leur activité sur la plateforme. Ce droit de portabilité[116] devra être octroyé à la demande de l'utilisateur final gratuitement et doit lui permettre d'avoir un accès en continu et en temps réel aux données[117].

— Assurer aux entreprises utilisatrices (et aux tiers autorisés par eux) un accès gratuit (et une utilisation effective) aux données fournies ou générées dans le cadre de l'utilisation des services de plateforme, y compris aux données agrégées. Les données à caractère personnel sont également visées[118]. Il est à noter que le règlement (UE) 2019/1150 prévoit déjà que tous les services d'intermédiation en ligne doivent inclure dans leurs conditions générales une description détaillée de l'accès (ou de l'absence d'accès) des entreprises utilisatrices aux données (personnelles ou autres) que les entreprises utilisatrices ou les consommateurs transmettent pour l'utilisation des services d'intermédiation[119].

— Offrir aux moteurs de recherche à des conditions équitables — et à leur demande — un accès aux données concernant les classements, requêtes, clics et vues générées par les utilisateurs finaux. Les données à caractère personnel devront être anonymisées[120].

— Communiquer gratuitement et quotidiennement à chaque annonceur à qui le contrôleur d'accès fournit des services de publicité en ligne (ou à un tiers désigné par l'annonceur), à sa demande des informations (le prix et les frais payés par l'annonceur, la rémunération perçue par l'éditeur et les mesures quantitatives à partir desquelles ces éléments sont calculés) relatives à chaque publicité mise en ligne. Le contrôleur d'accès devra également fournir des informations de même nature aux éditeurs à qui il fournit des services de publicité en ligne[121].

Par ailleurs, le DMA interdit aux contrôleurs d'accès d'utiliser — en concurrence avec une entreprise utilisatrice — les données qui ne sont pas accessibles au public et qui sont générées ou fournies par les entreprises utilisatrices dans le cadre de leur utilisation du service de plateforme essentiel ou qui sont fournies/générées par les clients des entreprises utilisatrices[122]. Il n'est pas anodin de relever qu'indépendamment du DMA, ce type d'interdiction se révèle également pertinent aux yeux des autorités de la concurrence ; ainsi cette interdiction figure-t-elle dans la communication de griefs que la Commission a envoyée à Meta dans le cadre de pratiques potentiellement contraires à l'article 102 du Traité sur le fonctionnement de l'Union européenne.[123] De même, dans le cadre d'une procédure d'enquête à charge d'Amazon, celle-ci a notamment offert un engagement de ne pas utiliser les données commerciales non publiques des vendeurs tiers utilisateurs de ses services de place de marché — engagement que la Commission a accepté le 22 décembre 2022. On se souviendra à ce sujet que l'enquête avait été ouverte précisément en raison du fait qu'Amazon utilisait les données commerciales non publiques de ses utilisateurs-vendeurs pour ajuster ses propres offres de vente, ce qui faussait la concurrence sur son site. Cette occurrence-ci a clairement inspiré l'insertion de la disposition précitée au sein du DMA.

Enfin, le DMA introduit à charge du contrôleur d'accès diverses interdictions visant en substance à empêcher l'extension de l'utilisation des données à caractère personnel obtenues par le contrôleur d'accès ou par des tiers[124]. Il ne peut être dérogé à ces interdictions que si l'utilisateur final y a consenti.

Dans la mesure où le respect de ces dernières interdictions est de nature à susciter des difficultés de contrôle dans le chef de la Commission, mais aussi des risques dans le chef du contrôleur d'accès, il se pourrait que l'utilisateur final soit régulièrement amené à donner son consentement à l'utilisation de ses données personnelles par le contrôleur d'accès.

17. Rappelons par ailleurs que le DMA permet à la Commission d'adopter des lignes directrices destinées à faciliter sa mise en œuvre et son application effective[125]. De plus, il est prévu que la Commission

(103) Article 19 du DMA.
(104) Article 3.2.a du DMA.
(105) Article 3.2.b et c du DMA.
(106) Article 3.4 du DMA.
(107) Article 3.5 du DMA.
(108) Article 17 du DMA.
(109) Articles 4.3 et 44 du DMA.
(110) Article 3.10 du DMA. Le délai de six mois commence à courir à compter de l'énumération d'un service de plateforme essentiel dans la décision de désignation. Celle-ci étant intervenue le 6 septembre 2023, le délai précité expirera donc le 6 mars 2024.
(111) Articles 6 et 7 du DMA.
(112) Article 8.2 du DMA.
(113) Article 5 du DMA.
(114) À l'exception de ce qui est prévu à l'article 6.11 qui ne vise que les moteurs de recherche.
(115) Communication du 19 février 2020, COM (2020) 66 final, p. 9.
(116) Ce droit de portabilité ainsi mis en place par le DMA prolonge le droit de portabilité des données à caractère personnel déjà prévu par le RGPD (article 20 du règlement 2016/679).
(117) Article 6.9 du DMA.
(118) Article 6.10 du DMA.
(119) Article 9 du Règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne *J.O.* L 186 du 11 juillet 2019, pp. 57-79.
(120) Article 6.11 du DMA.
(121) Article 5(9) et (10) du DMA.
(122) Article 6.2 du DMA.
(123) https ://ec.europa.eu/commission/presscorner/detail/en/ip_22_7728.
(124) Ces interdictions figurent à l'article 5(2) du DMA.
(125) Article 47 du DMA.

bénéficie d'une aide experte : le règlement charge la Commission de mettre en place un groupe de haut niveau[126] qui a pour mission de lui fournir des conseils et une expertise destinés à assurer une application cohérente du règlement, notamment au regard des différents autres instruments réglementaires (parmi lesquels le RGPD). Enfin, il reste à signaler que la Commission européenne dispose également en ce domaine de larges pouvoirs d'enquête, de coercition et de contrôle, qui lui permettent notamment d'infliger des amendes jusqu'à concurrence de 10 % du chiffre d'affaires total réalisé au niveau mondial au cours de l'exercice précédent[127].

5 Data Act (règlement (UE) 2023/2854)

18. Le « Data Act »[128], dont le texte a été publié récemment[129], est appelé à constituer une autre pièce maîtresse de l'édifice. Cet instrument a, lui aussi, pour objectif général de pallier le manque de disponibilité de données, tout en recourant à plusieurs voies qui lui sont spécifiques : il vise en effet (1) à instaurer un système de partage de données entre le fabricant d'un produit connecté à l'internet des objets (« IoT »)[130] (tel qu'un frigo ou un véhicule connecté, y inclus tout service essentiel intégré ou interconnecté sans lequel le produit ne pourrait pas remplir sa fonction) et l'utilisateur dudit produit (consommateur ou entreprise), (2) à créer un droit d'accès et d'utilisation pour le secteur public dans des situations exceptionnelles, (3) à faciliter le passage des services d'informatique en nuage aux services de traitement des données à la périphérie, (4) à mettre en place des garanties contre le transfert illicite de données par les fournisseurs de services informatiques en nuage et (5) à prévoir l'élaboration de normes d'interopérabilité pour les données qui seront utilisées entre les secteurs[131]. Nous ne traiterons dans la présente contribution que des trois premiers aspects.

19. S'agissant du partage de données générées par les produits IoT entre entreprises et consommateurs (B2C[132]) et entre entreprises (B2B[133]), voici comment se présente le règlement.

Le texte prévoit l'obligation de rendre accessibles les données générées par l'utilisation de produits connectés (en ce compris les assistants virtuels comme celui développé par Amazon sous le nom Alexa) et des services connexes[134]. À première vue, on pourrait penser que le champ d'application de ces dispositions est assez étroit mais il suffit de constater le nombre d'objets connectés pour comprendre que ce droit d'accès pourrait concerner un grand nombre de données générées dans le cadre de la vie courante (il suffit d'évoquer à titre d'exemples les frigos, les voitures, les systèmes d'alarme, les montres dotées d'applications liées à la santé). Le texte implique que dès le stade de la conception du produit, le fabricant doit veiller à ce que les données générées puissent, par défaut, être directement accessibles à l'utilisateur, d'une manière aisée, sécurisée et gratuite[135].

Le texte prévoit par ailleurs qu'avant la conclusion d'un contrat relatif à l'achat ou la location d'un produit connecté, l'utilisateur devra recevoir une information claire et précise concernant les données générées par le produit, notamment le type et le volume de ces données ainsi que la manière dont l'utilisateur peut y accéder[136]. Lorsqu'un utilisateur (ou une partie agissant en son nom) en fait la demande et que les données ne sont pas directement disponibles, le détenteur des données générées devra mettre celles-ci à la disposition du tiers indiqué par l'utilisateur (il pourrait s'agir, par exemple, d'un réparateur) ; cette mise à la disposition du tiers devra intervenir dans les meilleurs délais, sans frais pour l'utilisateur[137], en continu et en temps réel ; la disponibilité des données accordée au tiers devra être aisée et s'accompagner de la fourniture des métadonnées nécessaires à l'interprétation et à l'utilisation des données[138]. Le tiers en question ne pourra toutefois pas être le fournisseur d'un service de plateforme essentiel[139], c'est-à-dire l'opérateur désigné comme contrôleur d'accès conformément au DMA[140].

Les secrets d'affaires seront préservés et ne seront divulgués à des tiers que dans la mesure où ils sont strictement nécessaires pour atteindre la finalité convenue entre l'utilisateur et le tiers. Le détenteur des données (ou le détenteur des secrets lui-même si c'est une autre partie) identifiera les données qui sont protégées comme secrets d'affaires, et s'accordera avec le tiers pour déterminer toutes les mesures proportionnées de nature technique ou organisationnelle qui sont nécessaires pour préserver la confidentialité des données ainsi partagées (telles que des clauses contractuelles type, des accords de confidentialité, des protocoles d'accès stricts, des normes techniques et l'application de codes de conduite)[141]. Si les parties ne se mettent pas d'accord sur ces moyens ou si le tiers omet de mettre ces mesures en œuvre, ou encore s'il met à mal la confidentialité des données, le détenteur des données pourra refuser ou suspendre le partage des données. Dans ce cas, il avisera le tiers de sa décision dûment motivée et il adressera une notification à l'autorité compétente au niveau national[142].

Dans des circonstances exceptionnelles, le détenteur des données pourra également refuser, au cas par cas, la demande d'accès à des données spécifiques lorsqu'il pourra démontrer que la divulgation des secrets qu'elles constituent, est susceptible de lui causer un préjudice économique grave malgré les mesures techniques et organisationnelles prises par le tiers. En pareille hypothèse, il devra pouvoir fonder son refus sur des éléments objectifs liés en particulier à la nature et au niveau de confidentialité des données, à l'opposabilité de la protection des secrets d'affaires dans les pays tiers en cause, et au caractère unique et nouveau du produit concerné[143]. Le tiers disposera des moyens nécessaires pour contester une décision de refus d'accès aux données[144]. Indépendamment des recours qu'il peut exercer devant les juridictions nationales, il pourra saisir l'autorité nationale *ad hoc* qui doit être désignée par l'État membre ou des organismes certifiés de règlement des litiges[145] dont la mise en place est prévue par le règlement[146].

Le règlement prévoit encore d'autres restrictions au droit de l'utilisateur d'inviter le détenteur à accorder à un tiers l'accès aux données. Ainsi, ce droit ne pourra pas porter atteinte aux droits d'autres parties en matière de protection des données[147]. En outre, le tiers qui reçoit les données, ne pourra pas en disposer à sa guise puisqu'il ne pourra les traiter qu'aux fins et conditions convenues avec l'utilisateur, et dans le respect des droits de la personne concernée eu égard aux données à caractère personnel[148]. Il devra les effacer lorsqu'elles ne sont plus nécessaires à la finalité convenue[149].

(126) Article 40 du DMA. Ce groupe se compose des organes et réseaux européens suivant : l'organe des régulateurs européens des communications électroniques (BEREC) ; le Contrôleur européen de la protection des données et le Comité européen de la protection des données ; le réseau européen de la concurrence ; le réseau de coopération en matière de protection des consommateurs et le groupe des régulateurs européens pour les services de médias audiovisuels. Le 23 mars 2023, la Commission a annoncé avoir procédé à la création de ce groupe ; voy. https://digital-strategy.ec.europa.eu/en/news/digital-markets-act-commission-creates-high-level-group-provide-advice-and-expertise-implementation (consulté le 23 juin 2023).
(127) Article 30.1 du DMA.
(128) En français, le « règlement sur les données ».
(129) Voy. *supra*, note 31.
(130) Il s'agit ici du domaine dit de « l'internet des objets » (en anglais, « Internet of Things », en abrégé « IoT »).
(131) Article 1.1 du Data Act.
(132) Abréviation conventionnelle de « business to consumer ».
(133) Abréviation conventionnelle de « business to business ».
(134) Article 3 du Data Act.
(135) Article 3.1 du Data Act.
(136) Article 3.2 du Data Act.
(137) En revanche, le tiers devra payer une compensation raisonnable au détenteur des données. Voy. en ce sens, G. Monti, T. Tombal et I. Graef, 2022, *Study for developing criteria for assessing « reasonable compensation » in the case of statutory data access right : Study for the European Commission Directorate-General Justice and Consumers : final report*. EU Publications.
(138) Article 5.1 du Data Act.
(139) Article 5.3 du Data Act.
(140) Voy. *supra* concernant la notion de « contrôleur d'accès » et celle de « service de plateforme essentiel » dans le cadre du DMA. Observons cependant que si les contrôleurs d'accès ne sont pas éligibles comme bénéficiaires des données dans ce cadre-ci, ils pourraient recevoir des données en vertu du droit de portabilité consacré par le RGPD ; voy. à ce sujet, T. Tombal et I. Graef, *TILEC Discussion Paper*, « The regulation of access to personal and non-personal data in the EU : from bits and pieces to a system ? », novembre 2022, p. 11 (accessible en ligne à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4304148 ; dernière consultation : 19 juillet 2023).
(141) Article 5.9 du Data Act.
(142) Article 5.10 du Data Act.
(143) Article 5.11 du Data Act.
(144) Article 5.12 du Data Act.
(145) Article 5.12 du Data Act.
(146) Article 10 du Data Act.
(147) Article 5.13 du Data Act.
(148) Article 6.1 du Data Act.
(149) Article 6.1 du Data Act.

Un chapitre prévoit les conditions dans lesquelles les détenteurs de données mettent les données à la disposition des destinataires des données, en ce compris la compensation éventuelle (qui devra, en tout état de cause, être raisonnable), ainsi que les mécanismes destinés à assurer le règlement des litiges et les modalités techniques de protection éventuelles relatives à l'utilisation non autorisée de données. Par ailleurs, un chapitre distinct est consacré aux clauses contractuelles abusives imposées unilatéralement à une micro, petite ou moyenne entreprise[150].

L'exposé des motifs reconnaît que ce droit d'accès au bénéfice de l'utilisateur du produit connecté limite la liberté d'entreprise et la liberté contractuelle du fabricant ; il estime cependant que cette limitation se justifie au regard de la nécessité de renforcer la protection des consommateurs et en particulier de leur permettre de bénéficier d'un plus large choix de service après-vente : grâce au droit d'accès, l'utilisateur-consommateur cesserait en effet de dépendre exclusivement des services du fabricant[151]. On relèvera toutefois que l'obligation de partage ne s'applique pas aux données générées par l'utilisation de produits manufacturés (ou services liés) par des micro- ou petites entreprises[152].

Enfin, le projet vise également à clarifier — en le restreignant — le champ d'application du droit *sui generis* prévu par la directive sur la protection juridique des bases de données. Il prévoit en effet que ce droit ne s'appliquera pas aux bases de données contenant des données obtenues ou générées par l'utilisation de produits connectés ou services liés. L'objectif de l'exclusion est d'assurer que ce droit n'entrave pas l'accès, l'utilisation ou le partage des données que le règlement *Data Act* met en place[153].

20. Le règlement introduit ensuite un droit d'accès et d'utilisation pour le secteur public dans des situations exceptionnelles.

Plus précisément, le texte crée un cadre destiné à permettre aux organismes du secteur public[154] d'utiliser des données (ou des métadonnées nécessaires pour interpréter ou utiliser les données) détenues par des entreprises lorsqu'il existe un besoin exceptionnel et que les données ne peuvent pas être obtenues sur le marché en temps utile, de manière efficace et dans des conditions équivalentes. Les données devront être mises à disposition gratuitement lorsqu'il s'agira de répondre à une urgence publique (telle qu'une urgence de santé publique ou une catastrophe d'origine naturelle ou humaine comme une cyber attaque)[155]. Dans d'autres cas de besoin exceptionnel (par exemple prévenir ou contribuer au rétablissement d'une situation à la suite d'une urgence publique), le détenteur des données aura droit à une compensation (correspondant au remboursement des coûts techniques et organisationnels liés à la mise à disposition des données, majorés d'une marge raisonnable)[156]. À nouveau, les petites et micro-entreprises ne sont pas concernées par certaines formes de ce droit d'accès[157].

L'objectif de cette partie du projet de règlement est de permettre aux pouvoirs publics de prendre des mesures pour le bien commun tout en permettant au secteur privé de tirer profit de la rationalisation des procédures de demande des données. On peut supposer que dans certains cas, des discussions pourront surgir concernant les justifications de ce droit d'accès aux données, malgré les indications fournies par le texte sur ce qui constitue un besoin exceptionnel. Plusieurs cas de figure sont en effet envisagés où le besoin exceptionnel est réputé exister[158].

Dans un premier cas, le besoin exceptionnel est réputé exister lorsque les données sont nécessaires pour réagir à une urgence publique et que l'organisme public est incapable de les obtenir en temps opportun par une autre voie, en temps utile, d'une manière efficace et à des conditions équivalentes[159].

Dans un deuxième cas, le besoin exceptionnel est réputé exister lorsque les données sont nécessaires pour permettre à l'organisme public d'accomplir une mission légale d'intérêt public visant, par exemple, à établir des statistiques ou à réagir dans un second temps aux conséquences qui découlent d'une urgence publique, soit pour en limiter les effets soit pour contribuer au rétablissement de la situation[160]. Dans ce deuxième cas, l'organisme public ne peut bénéficier des données que s'il a épuisé toutes les voies alternatives pour les obtenir, notamment en les achetant sur le marché, ou en invoquant une obligation de les fournir ou en faisant adopter de nouvelles dispositions légales susceptibles de garantir leur mise à disposition en temps utile. Il devra justifier sa demande au regard de ces conditions et il devra apporter toutes les précisions telles qu'énoncées par le règlement[161]. En outre, s'agissant encore du deuxième cas de besoin exceptionnel, même si les conditions sont remplies, l'organisme public ne pourra obtenir les données que si celles-ci ne revêtent pas de caractère personnel[162].

De surcroît, le droit d'accès est soumis à des conditions plus strictes dans l'hypothèse où les données correspondent à des secrets d'affaires ou à des secrets d'affaires présumés : la communication des données ne peut être exigée que dans la mesure où elle est strictement nécessaire pour atteindre la finalité de la demande[163].

Sur le plan formel, la demande d'accès doit satisfaire à un certain nombre de conditions énoncées dans le règlement, ce qui oblige le demandeur à s'expliquer (notamment) sur la proportionnalité de la demande[164] en tenant compte de la protection des secrets d'affaires bénéficiant au détenteur des données[165]. Si la demande ne satisfait pas aux conditions qui lui sont imposées, elle peut faire l'objet d'un rejet ou d'une demande de modification de la part du détenteur des données[166]. Lorsque la demande concerne un ensemble de données dont certaines revêtent un caractère personnel, celles-ci devront en principe être anonymisées de manière adéquate. Toutefois, elles ne devront pas l'être si leur divulgation est nécessaire pour satisfaire à la demande de l'organisme public. Dans ce dernier cas, elles devront être pseudonymisées[167].

Par ailleurs, une fois l'accès obtenu, les organismes publics sont tenus de respecter certaines prescriptions dans l'utilisation qu'ils font des données : ils ne peuvent pas utiliser les données d'une manière incompatible avec la finalité pour laquelle elles ont été demandées ; ils doivent protéger les données à caractère personnel en mettant en œuvre des mesures techniques et organisationnelles garantissant les droits et libertés des personnes concernées ; ils doivent effacer les données lorsqu'elles ne sont plus nécessaires et ils doivent en informer le détenteur[168] ; ils ne peuvent effectuer la mise à disposition des données prévue par la directive 2019/1024 en vue de leur réutilisation par des tiers[169] ; ils ne peuvent pas utiliser les données en vue de développer un produit ou service concurrent à celui du détenteur de données[170].

On observera que si, dans l'hypothèse d'un besoin exceptionnel, le règlement limite de manière extrêmement stricte l'utilisation des données qui est autorisée, il en permet en revanche le partage lorsque celui-ci intervient pour des travaux de recherche scientifique (ou des analyses) ou avec des instituts nationaux de statistique (et Eurostat) en vue d'établir des statistiques officielles[171]. Encore faut-il, lorsque le partage intervient pour des travaux de recherche scientifique ou des analyses,

(150) Chapitres III et IV du projet Data Act.
(151) Pour une analyse critique de la justification de la création de ce droit, voy. A. Metzger et H. Schweitzer, « Shaping Markets : A Critical Evaluation of the Draft Data Act (September 18, 2022) », accessible en ligne à l'adresse : SSRN : https://ssrn.com/abstract=4222376 ou http://dx.doi.org/10.2139/ssrn.4222376, p. 7. Voy. également W. Kerber, « Governance of IoT Data : Why the EU Data Act will not Fulfill Its Objectives (Seconde Version) (July 18, 2022) », accessible en ligne (nouvelle version) à l'adresse suivante : GRUR International, ikac107, https://doi.org/10.1093/grurint/ikac107 (open access) ; également accessible en ligne (version antérieure) à l'adresse suivante : SSRN : https://ssrn.com/abstract=4080436 or http://dx.doi.org/10.2139/ssrn.4080436.
(152) Article 7 du Data Act.
(153) Article 43 du Data Act.
(154) Article 14 du Data Act. Le texte vise encore d'autres bénéficiaires, à savoir la Commission, la Banque centrale européenne ou un organe de l'Union.
(155) Article 20.1 du Data Act.
(156) Article 20.2 du Data Act.
(157) Article 15.2 du Data Act.
(158) Article 15 du Data Act (proposition).
(159) Article 15.1.a du Data Act.
(160) Article 15.1.b du Data Act.
(161) Article 17 du Data Act.
(162) Article 15.1b du Data Act.
(163) Article 19.3 du Data Act.
(164) Article 17.2.c du Data Act.
(165) Article 17.2.d du Data Act.
(166) Article 18.2 du Data Act.
(167) Article 18.4 du Data Act.
(168) Article 19.1 du Data Act.
(169) Article 17.3. Pour rappel, la directive 2019/1024 impose aux organismes du secteur public de mettre les informations qu'ils détiennent à la disposition des tiers, en format ouvert, et de permettre à ces tiers de réutiliser ces informations dans un autre but que le but de service général poursuivi par l'organisme public — que cet autre but soit commercial ou non ; voy. la contribution traitant de cette directive dans le prochain numéro du *Journal des tribunaux*.
(170) Article 19.2 du Data Act.
(171) Article 21.1 du Data Act.

que ceux-ci soient compatibles avec la finalité pour laquelle les données ont été demandées par l'organisme public.

Dernière précision d'importance : le système conçu par le règlement ne s'applique pas aux interventions des organismes publics dans le cadre des poursuites et des sanctions pénales ou administratives, celles-ci étant soumises à un régime particulier qui n'est pas affecté par le règlement[172].

21. Enfin, le règlement instaure un dispositif destiné à faciliter le passage des services d'informatique en nuage aux services de traitement de données à la périphérie.

Cette partie du règlement vise à améliorer la situation des entreprises clientes des services d'informatique en nuage (en anglais, « cloud »), et à leur préserver la possibilité de changer de fournisseur[173].

En particulier, ces « fournisseurs de service de traitement de données » en nuage doivent supprimer les obstacles qui freinent leurs clients dans la résiliation de leurs contrats, par exemple, un délai de préavis excessif pour le lancement du processus de changement de fournisseur ou, en cas de changement de fournisseur, un délai insuffisant pour la récupération des données auprès du fournisseur initial[174]. À cet égard, le contrat devra prévoir un délai maximal de préavis pour le lancement du processus de changement de fournisseur, qui ne dépasse pas deux mois[175], ainsi qu'une période minimale d'au moins trente jours calendaires pour la récupération des données[176]. Il devra également prévoir que le fournisseur initial fournit une assistance raisonnable dans le cadre du processus de changement de fournisseur et qu'il agit avec diligence pour maintenir la continuité des activités et la poursuite des fonctions ou services[177]. Parmi les autres mesures destinées à faciliter le changement de fournisseur, le règlement énonce qu'à compter du 12 janvier 2027, le client ne peut se voir imposer aucun frais pour le processus de changement[178].

De manière générale, le règlement impose à toutes les parties impliquées de coopérer de bonne foi pour rendre le processus de changement de fournisseur effectif, permettre en temps utile le transfert des données et maintenir la continuité du service de traitement des données[179]. Sur le plan technique, le règlement vise à permettre à l'utilisateur de bénéficier d'une équivalence fonctionnelle dans l'utilisation du service après le changement de fournisseur[180] et, s'agissant de certains types de services, à mettre à la disposition du public des interfaces ouvertes[181]. Des dérogations sont prévues pour des applications de stockage qui sont conçues sur mesure en fonction des besoins spécifiques d'un client individuel et qui ne sont pas offertes à une large échelle commerciale[182].

22. Il reste à évoquer brièvement les règles que le règlement prévoit à propos de la désignation des autorités compétentes.

Chaque État membre doit désigner une ou plusieurs autorités compétentes chargées de l'application du Data Act. Il peut s'agir soit d'une nouvelle autorité soit d'une autorité existante[183]. Lorsqu'un État membre désigne plusieurs autorités, il devra désigner un « coordinateur de données » qui aura pour mission de faciliter la coopération entre les autorités compétentes et de fournir une assistance aux entités visées par le Data Act[184].

Le règlement précise toutefois que les questions spécifiques relatives au traitement des données à caractère personnel relèveront de la responsabilité des autorités de contrôle indépendantes chargées de contrôler l'application du règlement 2016/679 sur les données à caractère personnel (le RGPD)[185].

Par ailleurs, il prévoit que l'autorité à désigner doit disposer d'une expérience dans le domaine des données et des services de communications électroniques pour ce qui concerne le volet relatif au changement de fournisseur de services de traitement des données[186].

Parmi les missions qui lui sont confiées, l'autorité à désigner devra notamment sensibiliser les utilisateurs et les entités visées aux droits et obligations issus du règlement, traiter les réclamations (en ce compris sur des questions liées aux secrets d'affaires[187]) et imposer des sanctions financières. Le règlement traite également la question de l'intervention des juridictions nationales à l'encontre des décisions prises par l'autorité compétente. Il prévoit qu'indépendamment de toute possibilité d'un recours administratif ou d'un autre recours non juridictionnel, toute personne affectée par une décision contraignante de l'autorité compétente dispose du droit à un recours effectif[188] devant les cours et tribunaux de l'État membre de l'autorité en cause[189].

6 Quelques constats en guise de conclusion

23. Malgré l'annonce en 2020 d'un programme cohérent lorsque la Commission a dévoilé sa stratégie pour les données, les instruments législatifs élaborés par la suite ont contribué à créer un cadre particulièrement complexe[190] et en apparence quelque peu décousu.

Plusieurs observations retiennent l'attention à cet égard. Premièrement, même si les champs d'action des trois initiatives commentées dans la présente contribution sont distincts, il n'est pas absolument certain que tout risque de chevauchement soit exclu[191]. En outre, si les ambitions de chacun des textes sont indéniables, les interrogations ne manquent pas quant aux bénéfices effectifs que l'on peut en espérer.

Ainsi, le DGA vise à faciliter l'accès par le secteur privé aux données détenues par le secteur public et à introduire un cadre normatif pour les services d'intermédiation des données dans le but de faciliter le partage de données à titre altruiste. Ce dernier mécanisme en particulier suscitera une certaine perplexité aussi longtemps qu'il n'aura pas donné lieu à des mises en pratique convaincantes.

Le DMA, en apparence plus simple, vise quant à lui à imposer aux géants de l'internet une obligation de partage de données et un grand nombre d'interdictions d'utilisation des données générées par l'utilisation de leurs plateformes. Les modalités de mise en application de ce système s'annoncent néanmoins très compliquées et la Commission devra développer des compétences techniques non négligeables afin d'assurer une mise en œuvre effective et continue de l'ensemble.

La dernière pierre de l'édifice, le Data Act, poursuit des objectifs de partage particulièrement ambitieux dès lors que pour la première fois, le secteur public se voit attribuer le droit d'exiger un accès à des données détenues par le secteur privé. Ici aussi, les interrogations ne manquent pas tant les sujets de discussions potentiels paraissent nombreux et délicats, notamment en ce qui concerne la proportionnalité de la demande d'accès de la part de l'organisme du secteur public, le respect des intérêts légitimes du détenteur des données ou la compensation éventuelle que ce dernier pourrait revendiquer.

À cela s'ajoute que le succès du dispositif général mis en place par la Commission dépend aussi en grande partie des moyens qui seront déployés au plan national[192]. L'action concrète des autorités compétentes qui doivent être désignées par chaque État membre est en effet

(172) Article 16.2 du Data Act. Comme l'indique le dixième considérant du Data Act, le régime particulier applicable en ces matières figure notamment dans les réglementations suivantes : le règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion de contenus à caractère terroriste en ligne, les textes relatifs à l'accès aux preuves électroniques en matière pénale, le 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) (DSA), ainsi que de la coopération internationale dans ce domaine fondée, en particulier, sur la convention de 2001 du Conseil de l'Europe sur la cybercriminalité (« convention de Budapest »).
(173) Chapitre VI du Data Act.
(174) Articles 23 et 25 du Data Act.
(175) Article 25.2.d du Data Act.
(176) Article 25.2.g du Data Act.
(177) Article 25.1.a du Data Act.
(178) Article 29.1 du Data Act.
(179) Article 27 du Data Act.
(180) Article 30.1 du Data Act.
(181) Article 30.2 du Data Act.
(182) Article 31.1 du Data Act.
(183) Article 37.1 du Data Act.
(184) Article 37.2 du Data Act.
(185) Article 37.3 du Data Act.
(186) Article 37.4 du Data Act.
(187) Article 37.5.b du Data Act.
(188) Article 39.1 du Data Act.
(189) Article 39.3 du Data Act.
(190) Le cadre devient encore plus complexe si on y ajoute les initiatives sectorielles à venir (les « Common European Data Spaces ») telles que la proposition relative au Health Data Space (EHDS).
(191) Ainsi, tout risque de chevauchement n'est pas radicalement exclu entre le DMA et le Data Act en ce qui concerne les assistants virtuels.
(192) En tout cas en ce qui concerne le DGA et le Data Act qui confient aux États membres le soin de désigner les autorités compétentes. En revanche, pour ce qui est du DMA, c'est la Commission qui est seule compétente.

largement tributaire des ressources techniques et financières qui seront mises à leur disposition.

D'une manière plus générale, on ne peut s'empêcher de se poser la question — probablement naïve : pourquoi l'Union ne s'est-elle pas dotée d'un corpus législatif unique susceptible de réglementer le droit des données dans son ensemble, d'une manière cohérente et aisément lisible ? Il s'agit là d'une question qui prolonge un vœu universel bien connu dans la communauté des juristes praticiens. Aussi légitime que soit cette question, elle ne saurait cependant conduire à ignorer la nécessité de procéder par étapes quand on a affaire à une problématique (les données) qui se distingue tant par son évolution constante que par ses ramifications multiples. Certes, il n'est pas inconcevable qu'à terme, un code unique puisse voir le jour, qui réunirait les réglementations des différentes composantes de la matière. Mais à ce stade-ci, ce résultat semble encore éloigné. De là le point d'interrogation qui, dans le titre de la présente contribution, interroge le caractère global du cadre réglementaire mis en place par l'Union.

Michèle LEDGER
Maître de conférences à l'UNamur, chercheuse au CRIDS-NADI
Benoît MICHAUX
Professeur à l'UNamur, chercheur au CRIDS-NADI