La libre circulation des données est devenue la cinquième liberté consacrée dans le droit de l'Union européenne

Description

Ainsi en dispose le règlement européen adopté le 14 novembre 2018[1], qui établit un cadre applicable à cette nouvelle liberté s'agissant des données non personnelles. Ce texte complète le RGPD (Règlement général sur la protection des données), qui prévoit également le principe de cette libre circulation à l'égard des données personnelles (art. 1er § 3).

L'adoption de ce texte s'inscrit dans le cadre de la stratégie pour un marché unique numérique proposée par la Commission européenne. L'un de ses objectifs consiste à créer un cadre juridique et politique adapté pour l'économie fondée sur les données[2], l'exploitation de celles-ci constituant une nouvelle « révolution industrielle[3] ».

De nombreux services innovants reposant sur ces ressources sont en effet voués à se développer, notamment sur les marchés des objets connectés et des villes « intelligentes ». L'ouverture des données publiques, ou *Open Data*, doit également permettre de doper l'économie des données. Comme l'indique le règlement dans son préambule, de multiples activités ont permis de constituer de nouvelles chaînes de valeur basées sur l'exploitation des données : création et collecte, agrégation et organisation, traitement, analyse, commercialisation et distribution, utilisation et réutilisation. De telles actions d'exploitation au sein du marché unique numérique supposent naturellement la libre circulation des données au sein des États membres. C'est pourquoi, le règlement du 14 novembre 2018 vise principalement à faire tomber les barrières à cette libre-circulation et à organiser la coopération entre les États membres concernant l'accès à ces données.

Le champ d'application : les traitements de données non personnelles

Le champ d'application du nouveau règlement est particulièrement large, tant au regard des définitions qu'il pose que des actes qu'il vise. Les données non personnelles sont ainsi définies comme toutes les données autres que celles à caractère personnel visées par l'article 4 du RGPD (voir *La rem* n°42-43, p.21). Cette définition résiduelle a l'avantage de couvrir un grand nombre de données brutes, aussi bien publiques que privées, leur principale caractéristique étant de ne pas pouvoir être reliées à des personnes physiques. Les traitements de données non personnelles sont également définis, de manière identique à celle du RGPD, comme incluant *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données sous forme électronique »*. Selon les articles 1 et 2 du règlement, le principe de libre circulation est donc voué à s'appliquer à de telles opérations lorsqu'elles sont fournies en tant que services aux utilisateurs résidant ou disposant d'un établissement dans

l'Union par un fournisseur de services qui y est lui-même établi, ou bien simplement si elles sont effectuées par une personne établie dans l'Union pour ses propres besoins. Les utilisateurs de tels traitements peuvent être aussi bien des personnes physiques que des personnes morales publiques ou privées, et réaliser ceux-ci à des fins professionnelles ou personnelles.

Le règlement prévoit également une articulation avec le RGPD lorsqu'un même ensemble de données comprend à la fois des données personnelles et des données non personnelles. La question est essentielle, parce que chaque catégorie de données est soumise à des régimes juridiques différents, celui qui s'applique aux données personnelles étant bien entendu plus contraignant pour les responsables du traitement de données. Ainsi, lorsque les données personnelles et non personnelles restent dissociables au sein d'un même ensemble, chaque règlement s'appliquera à la catégorie qu'il vise. Néanmoins, si les données sont indissociables, il est précisé que le nouveau règlement s'appliquera sans préjudice du RGPD, ce qui semble logique et particulièrement essentiel dans la pratique. On sait en effet qu'un certain nombre de données peuvent ne pas être personnelles au moment de leur collecte mais acquérir ultérieurement ce caractère par croisement, agrégation ou regroupement. Tel pourrait être le cas avec les traitements effectués dans le cadre des villes « intelligentes », où la réunion et l'analyse de fichiers de données brutes peuvent impliquer un risque dit de « réidentification[4] ».

Le RGPD devrait donc conserver la primauté dans toutes les hypothèses où sont traités des ensembles comportant une série de données personnelles, quand bien même celles-ci n'y occuperaient qu'une part minoritaire.

La disparition des exigences de localisation des données

Afin de garantir la libre circulation des données, le règlement entend faire tomber les « barrières » nationales numériques qui pourraient contrarier celles-ci. L'article 4 prévoit ainsi l'interdiction des exigences de localisation des données, assimilables à de véritables « contrôles aux frontières » numériques. Le règlement entend en l'occurrence toutes les dispositions prévues par des États membres, quelle que soit leur nature (légale, réglementaire, administrative…), qui ont pour objet ou pour effet d'imposer un stockage local des données sur leur territoire national ou sur une zone géographique précise. Celles-ci peuvent résulter par exemple de l'obligation d'employer certains moyens techniques certifiés ou agréés dans un État membre particulier (cf. § 4 du préambule). Outre l'interdiction d'adopter de telles mesures pour l'avenir, le règlement met en demeure les États membres de supprimer toutes celles qui sont encore en vigueur d'ici au 30 mai 2021. Ces contraintes apparaissent désuètes alors que les techniques d'informatique « dans les nuages » permettent justement de multiplier les accès aux données, d'en garantir la pérennité et de favoriser leur libre circulation. On sait bien sûr que la référence « aux nuages » n'est qu'une métaphore, les données étant nécessairement stockées dans un *datacenter* physiquement établi sur le territoire d'un État[5]. Or, la frilosité de certains États et les initiatives en faveur d'un *cloud* « souverain » visaient justement à éviter la délocalisation de données sur des territoires où elles seraient prétendument moins accessibles et moins sécurisées.

De telles objections ne seront plus opposables par les États, l'objectif principal du règlement consistant à ouvrir la concurrence entre services de *cloud computing* au niveau européen, tant pour les données des entreprises privées que pour celles des institutions publiques.

L'exception à la libre circulation : la sécurité publique

Le préambule du règlement ne laisse aucun doute quant à l'ouverture du marché aux données publiques. Il précise à cet égard que les autorités publiques et autres organismes de droit public doivent disposer d'une *« plus grande liberté de choix pour ce qui est des fournisseurs de services axés sur les données, de prix plus concurrentiels »* (§ 13). Le stockage de données issues des institutions administratives de l'État ou d'autres personnes morales de droit public pourra donc être effectué hors des frontières de leur territoire national. À ce niveau, le règlement ne prévoit qu'une seule exception au principe de libre circulation.

Cette dernière ne pourra être restreinte que pour des motifs de sécurité publique, dont les États membres auront à rendre compte devant la Commission européenne (art. 4). Si le texte est assez succinct quant à la nature de ces motifs, le préambule fournit d'intéressantes précisions qui tendent à en réduire la portée. Le concept de sécurité publique ne peut ainsi être entendu que comme la *« sécurité intérieure ou extérieure d'un État membre »*, la *« détection des infractions pénales »*, les poursuites et enquêtes. Il présuppose également l'existence d'une *« menace réelle et suffisamment grave portant atteinte à l'un des intérêts fondamentaux de la société »*, tel le fonctionnement des institutions ou des services publics essentiels, ou *« pour la survie de la population »*, le *« risque d'une perturbation grave des relations extérieures ou de la coexistence pacifique des nations »* ou encore un *« risque pour les intérêts militaires »* (§ 19). Les exigences de localisation des données sur un territoire national devront donc être réduites au strict minimum au regard de ces objectifs.

La coopération entre États membres concernant l'accès aux données

Le règlement prévoit également un encadrement des mesures d'accès aux données que pourraient ordonner les États, celles-ci ne pouvant concerner que des atteintes minimales au principe de libre circulation.

La question est essentielle au titre des enquêtes que pourraient mener les autorités publiques et qui nécessiteraient l'accès et la consultation de données stockées hors de leurs frontières. Elle rappelle que les États membres conservent une relative souveraineté numérique sur les données produites par les entreprises ou les institutions établies sur leur territoire national. Cette problématique, qui avait pu être soulevée en matière de données personnelles[6], vaut également pour les données non personnelles. Les articles 5 et 7 organisent ainsi la disponibilité des données pour les autorités compétentes. Chaque État membre sera tenu de créer en son sein un point de contact unique chargé de recevoir et d'instruire les demandes d'accès aux données sollicitées par les autorités des autres États. Ces derniers pourront exiger la relocalisation des données sur leur territoire pour une durée maximale de 180 jours. Tout dépassement devra être notifié à la Commission pour examen de compatibilité. Les points de contact uniques pourront également adresser des

lignes directrices aux utilisateurs concernés par le règlement.

Le portage des données pour les utilisateurs professionnels

Enfin, le règlement entend faire tomber une deuxième série d'obstacles à la libre circulation en organisant le portage des données par les utilisateurs professionnels (art. 6). Cette notion est bien sûr à rapprocher du principe de « portabilité » consacré par le RGPD pour les données personnelles.

L'objectif est de mettre un terme aux situations de dépendance vis-à-vis des fournisseurs de services de *cloud computing*, ceux-ci étant en mesure d'imposer des standards techniques qui leur sont propres et qui limitent la liberté de choix des utilisateurs. Une approche souple est ici retenue par le règlement, puisqu'il renvoie à l'élaboration de codes de conduite censés garantir les bonnes pratiques en termes de transparence et d'interopérabilité des traitements de données non personnelles (standardisation des formats, délivrance d'informations précontractuelles, dispositifs de certification…).

Perspectives en droit français

En l'état actuel, la conformité du droit français aux exigences du règlement apparaît relativement contrastée. Si les standards actuels de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) autorisent déjà un stockage au sein de l'Union européenne aux prestataires de services de *cloud computing*[7], la portée de l'exception de sécurité publique est susceptible de se heurter à certaines difficultés. On peut imaginer que celle-ci pourra concerner les données relevant de certains secteurs d'activité et acteurs tels que les opérateurs d'importance vitale (art. L 1332-1 du code de la défense) ou les opérateurs de services essentiels (loi du 26 février 2018). Cependant, les exigences posées en matière de localisation des archives publiques ne devraient pas être couvertes par cette exception.C'est pourtant ce que demandent les ministères de l'intérieur et de la culture et de la communication dans une note du 5 avril 2016 concernant les archives des collectivités territoriales[8]. Par une interprétation relativement imaginative selon Noé Wagener[9], cette note rappelle que les archives publiques sont des trésors nationaux au sens de l'article L 111-1 du code du patrimoine, le régime juridique applicable à cette catégorie de biens excluant leur exportation hors du territoire national. Sur cette base, la note précise que le recours à une offre de *cloud* non souverain est illégal et que les collectivités devront s'orienter exclusivement vers des offres garantissant un stockage local.

On ne peut que douter de la compatibilité de cette argumentation au règlement. Certes, des motifs de sécurité sont bien à la base de ce régime d'interdiction d'exportation, mais ils ne relèvent pas *a priori* de ceux qui sont visés par le texte européen. Cela est d'autant plus vrai que les trésors nationaux sont appréhendés par le code du patrimoine dans leur dimension strictement matérielle et non sous une forme numérique. On ne voit donc pas pourquoi la numérisation et le stockage des archives hors du territoire seraient incompatibles avec le respect de l'interdiction d'exportation, qui ne concerne que le support matériel.

Le règlement s'appliquera à partir du 19 juin 2019 et la France aura donc jusqu'au 30 mai 2021 pour

soustraire le droit national à telles exigences de localisation.

Sources :

1. Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.
2. Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Créer une économie européenne fondée sur les données », 10 janvier 2017.
3. Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Vers une économie de la donnée prospère », 2 juillet 2014.
4. « Données personnelles : les risques liés aux *Smart Cities* », *Expertises des systèmes d'information*, Philippe Mouron, mars 2017, p. 103-107.
5. « La définition des contours juridiques du *Cloud computing* », Emmanuel Sordet et Richard Milchior, Communication-Commerce électronique, n° 11, 2012.
6. Voir « Le *Cloud computing* à l'épreuve des souverainetés nationales – Faut-il avoir peur du *USA Patriot Act ?* », Béatrice Delmas-Linel et Céline Mutz, RLDI, n° 90, février 2013, p. 53-59 ; Flora Plénacoste et Emmanuel Daoud, « *Could Act* : des inquiétudes légitimes », *Dalloz IP/IT*, 2018, p. 680.
7. Prestataires de services d'information en nuage (SecNumCloud) – Référentiel d'exigences, ANSSI, version 3.1 du 11 juin 2018, § 19.2.
8. Note d'information du 5 avril 2016 relative à l'informatique en nuage (*cloud computing*), DGP/SIAF/2016/006.
9. « *Cloud* souverain et archives publiques », Noé Wagener, *Juris Art etc.*, février 2017, p. 38-41.

Categorie

1. Droit

date créée
19 mars 2019
Auteur
philippemouron