Numérique - La conservation des données, quels enjeux pour la souveraineté numérique ? - Etude par Pauline Türk

La Semaine Juridique Administrations et Collectivités territoriales n° 50, 19 décembre 2022, 2348

La conservation des données, quels enjeux pour la souveraineté numérique ?

Etude par Pauline Türk professeur de droit public à l'université Côte d'Azur, CERDACFF

Si le concept de souveraineté numérique, très à la mode, fait l'objet de plusieurs acceptions, il renvoie en premier lieu à la capacité de l'État de faire respecter son autorité et de défendre ses intérêts dans l'espace numérique. Les réglementations et pratiques relatives à la conservation des données interrogent précisément le rôle et la marge de manœuvre des États face à l'Union européenne et aux acteurs privés, alors que les enjeux économiques, politiques, de santé et de sécurité s'amplifient.

1. - Le concept de souveraineté numérique s'impose depuis une décennie mais fait l'objet d'acceptions diverses[Note 1]. Une première conception est juridique et renvoie, classiquement, à la souveraineté des États[Note 2]. Peuvent-ils prétendre réguler l'espace numérique comme ils réglementent l'espace physique délimité par leurs frontières ? Peuvent-ils prolonger leur pouvoir légitime de commandement sur les réseaux numériques ? Cela implique la production de normes qu'ils entendent pouvoir déployer, la capacité à fixer les règles, à faire respecter leurs lois, à protéger leurs citoyens dans l'espace numérique. L'exercice de leur autorité implique aussi la conduite de politiques industrielles et de développement technologique, dont dépendent leur aptitude à défendre et promouvoir leurs intérêts et leurs valeurs dans le champ du numérique. Cependant, tous les États n'ont pas la même puissance pour y parvenir, et ne poursuivent pas tous les mêmes objectifs. *« Reconquérir la souveraineté numérique »* pour la France, l'Allemagne, le Brésil, la Chine, l'Iran, ou la Russie ne renvoie pas du tout aux mêmes préoccupations. L'État peut viser la protection ou bien la surveillance des citoyens, il peut défendre la liberté sur les réseaux ou au contraire chercher à en encadrer strictement l'utilisation. Surtout, la revendication par les États de leur souveraineté numérique vient heurter une conception libertarienne déjà ancienne qui entendait construire un nouveau monde virtuel échappant à l'emprise des États et de leurs *« gouvernements de chair et d'acier »*[Note 3]. La perspective d'un découpage des espaces numériques en zones d'influence des États apparaît bien contraire au projet initial d'un internet ouvert. Mais la montée en puissance de la technologie numérique dans tous les secteurs d'activités et la domination de certains acteurs américains ou asiatiques sur le marché ont eu raison des projets les plus idéalistes, et ont accru les revendications de certains États tendant à gouverner leur *« portion »* de l'espace numérique. L'organisation d'une gouvernance mondiale multipartite des réseaux, incluant les États, a été discutée dès les premiers sommets mondiaux pour la société de l'information, puis lors des forums annuels sur la gouvernance de l'internet[Note 4].

2. - Une deuxième approche de la souveraineté numérique peut être qualifiée de libérale, et renvoie à la souveraineté des utilisateurs, des citoyens à l'ère numérique. Le citoyen a-t-il un droit de regard sur la gouvernance du monde numérique ? Est-il, individuellement (en tant qu'utilisateur de la technologie) ou collectivement (en tant que membre d'une communauté d'utilisateurs), capable de s'autodéterminer dans l'espace numérique ? De la même façon que le citoyen dans le *« Contrat social »* rousseauiste était un co-souverain, détenteur d'une fraction de la souveraineté, ce qui lui donnait le droit de contribuer à l'élaboration des règles communes, l'utilisateur membre de la société numérique devrait pouvoir maîtriser son destin, contribuer à la détermination des règles applicables, et voir protéger ses libertés. Dans une approche collective, les peuples souverains se choisissent des gouvernants chargés de gouverner dans l'intérêt général et tenus de rendre des comptes de leur action. Mais si les véritables gouvernants, à l'ère numérique, ne sont plus les institutions politiques élues, alors la souveraineté numérique implique une meilleure maîtrise par des communautés d'utilisateurs, potentiellement transnationales, des conditions de cette gouvernance. Dans une approche individuelle, le citoyen devrait bénéficier des droits et libertés qui sont la contrepartie de l'obéissance aux règles communes, et garder la maîtrise de son destin numérique, possiblement en lien avec le concept d'*« autodétermination informationnelle »* garanti par certaines cours constitutionnelles et par la Cour de Strasbourg[Note 5].

3. - Enfin, une troisième conception de la souveraineté numérique, utilisée dans la sphère politique, économique, médiatique, renvoie au pouvoir de certains opérateurs économiques, qui disposent *de facto* de la capacité à gouverner et à se faire obéir. Parlant d'égal à égal avec les États, dotés d'une puissance financière parfois supérieure à eux, ces opérateurs privés jouissent d'une situation de quasi - monopole leur permettant de régner sur les marchés et d'imposer leurs conditions. Ces multinationales exercent une forme de pouvoir normatif, fixent les conditions générales d'utilisation (CGU), créent leurs propres organes de règlement des différends, imposent leurs valeurs en matière de liberté d'expression, exploitent les données des utilisateurs, échappent aux lois et à l'impôt. Elles rivalisent même avec les États dans la fourniture de certains services (monnaies virtuelles, effets de la plateformisation de l'économie et de l'administration, développement des outils numériques au service de la justice, la police, la santé...). Certains leaders de ces multinationales ne cachent pas leur prétention à diriger le monde de demain, voire à remplacer les États, grâce aux services rendus dans de nombreux domaines. Dire que les multinationales, notamment les GAFAM américaines, exercent une forme de souveraineté, c'est reconnaître que leur position dominante leur donne une puissance, un pouvoir de s'imposer et de se faire obéir, de peser dans la gouvernance de l'activité des communautés humaines, presque d'égal à égal avec les États.

4. - Ces trois principales approches n'épuisent pas la notion, puisqu'on entend parler de souveraineté numérique industrielle, technique ou technologique. Et au sens juridique, la souveraineté numérique ne serait plus seulement celle des États, puisqu'il est question, désormais, de souveraineté numérique européenne[Note 6], à l'heure où l'Union multiplie les initiatives et réglementations pour reprendre la maîtrise du destin numérique de ses citoyens, comme l'illustre par exemple l'élaboration des *Digital Market Act* et *Digital service Act* en 2022.

5. - La question des conditions de recueil, de stockage, de conservation et de traitement des données est un des enjeux majeurs des débats sur la souveraineté numérique. L'exploitation généralisée des données de connexion intéresse les États membres de l'Union européenne, en réponse à la menace terroriste, fragilisant l'équilibre entre sécurité et liberté. Parallèlement, la pandémie de Covid-19 a accentué la politique de surveillance au travers d'applications de contact tracing et de contrôle de la circulation, dans le cadre d'une délicate conciliation entre respect de la vie privée et sauvegarde de la santé publique. Le traitement algorithmique des données fonde un nombre grandissant de décisions publiques et privées. Le développement des législations extra-territoriales a accentué le risque de contournement des dispositifs de protection des données[Note 7]. La dépendance technologique aux géants du numérique n'a pas été corrigée. Le potentiel économique et industriel des données aiguise les appétits.

Dans ce contexte, les États cherchent à reprendre le contrôle, à bâtir des *« solutions souveraines »*, à rapatrier ou à attirer les data centers, à soutenir leurs quelques licornes et start-up prometteuses... Dans le même temps, l'Union européenne œuvre à parachever, après le RGPD, puis le règlement sur la libre circulation des données non personnelles[Note 8], la création d'un vaste marché ouvert de la donnée, par la consécration d'une cinquième liberté de circulation[Note 9]. Dans l'*« espace Shengen de la donnée »*, la libre circulation des données est la règle et les exceptions ne peuvent être que strictement limitées et justifiées par des impératifs de sécurité.

Sur le terrain de la conservation des données, l'un des enjeux consiste à s'accorder sur l'échelon auquel la réglementation doit être édictée et sur les marges d'action respectives des États et de l'Union européenne en la matière. Des contentieux récents ont révélé des tensions relatives à la capacité dont disposent ou non les États à réglementer les conditions de la conservation des données, du fait de leur intégration dans l'Union européenne (**1**). L'autre perspective conduit à envisager la façon dont l'Union européenne parvient - ou non - à maîtriser le destin des citoyens européens vis-à-vis des interventions extérieures, d'autres États, d'opérateurs économiques, ou encore d'entités malveillantes (**2**). Sous l'angle de la réglementation de la conservation des données, c'est bien la souveraineté numérique dans son rapport à l'État dont il est ici question.

1. La souveraineté numérique de l'État en matière de conservation des données au sein de l'Union européenne

6. - La souveraineté numérique des États est habituellement confrontée à la puissance technologique ou économique d'acteurs privés qui viennent interférer dans l'exercice de leur autorité. Mais certaines limites proviennent, pour les États membres, de l'intégration dans l'Union européenne, dont la réglementation limite la capacité des États à fixer leurs propres règles en matière de conservation des données. L'article 16 du Traité sur le fonctionnement de l'Union européenne prévoit en effet, outre la garantie de la protection des données à caractère personnel déjà incluse à l'article 8 de la Charte des droits fondamentaux de l'Union européenne, que les règles *« relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données »* sont fixées par le Parlement européen et le Conseil conformément à la procédure législative ordinaire. On peut prendre deux exemples de ces restrictions imposées aux États dans la détermination des règles relatives à la conservation des données, qui mettent donc en jeu leur « souveraineté numérique ». Il s'agit de protéger une conception exigeante de la liberté individuelle face à des dispositifs nationaux de sécurité potentiellement invasifs (**A**), mais aussi de protéger la logique de marché ouvert et d'éliminer les barrières nationales à la circulation des données, faisant obstacle au développement à l'échelle nationale de solutions de *cloud* souverain (**B**). Ces questions peuvent être abordées à la lumière des tensions relatives aux marges résiduelles de souveraineté des États membres, à la suite de décisions des juges nationaux, britannique et français, mais aussi allemand ou polonais qui ont été largement commentées[Note 10].

A. - La capacité de l'État à décider de la conservation généralisée des données pour motif de sécurité nationale

7. - La restriction de la possibilité pour un État d'imposer aux opérateurs la conservation généralisée et durable des données numériques illustre une première limite à sa souveraineté numérique, au sein de l'Union européenne. Les gouvernements nationaux sont confrontés au terrorisme, chargés de lutter contre toutes les formes de délinquance, contre les réseaux de criminalité, et d'assurer la sécurité intérieure. Ils ont besoin de disposer de tous les moyens utiles pour améliorer l'efficacité des services de police et de justice. Bien sûr, la conservation durable des données numériques constitue un outil précieux à cet égard. Or, la directive européenne *Privacy* de 2002-1958 interdit, par principe, la conservation généralisée des données de connexion et n'admet d'exception qu'en cas de menace grave pour la sauvegarde de la sécurité nationale, dans des conditions qui ont été encadrées par la Cour de justice de l'Union[Note 11]. En matière de lutte contre le crime, ne sont conformes au droit de l'Union que les dispositifs nationaux prévoyant une conservation ciblée et strictement encadrée. Encore faut-il préciser que ces dispositifs ne sont validés que dans le cadre de la lutte contre les formes de criminalité les plus graves, la recherche des auteurs d'infractions n'entrant pas dans ce périmètre.

C'est bien la question de la souveraineté numérique de l'État qui transparaît, en avril 2021, dans « l'affaire French data network », sous l'angle du droit pour un État de prévoir les conditions de conservation des métadonnées numériques de ses citoyens[Note 12]. Le gouvernement français défendait le maintien d'une conservation généralisée pendant un an, par les fournisseurs d'accès et hébergeurs de contenus, des données de connexion, à savoir les données de trafic et de localisation des utilisateurs, afin de pouvoir y accéder en cas de besoin lié à une enquête pénale ou aux activités de renseignement. Or, selon la jurisprudence européenne, de tels motifs ne justifient qu'une conservation ciblée et strictement encadrée des données et seulement lorsque sont concernées les formes les plus graves de criminalité. L'arrêt rendu en assemblée le 21 avril 2021 a fait grand bruit dans la mesure où le Conseil d'État fait prévaloir des exigences constitutionnelles spécifiques pour valider le dispositif national en cause et justifier la conservation générale et durable des données pour les besoins de la sécurité nationale et de la poursuite des infractions d'un degré de gravité suffisant. Il considère en effet que l'encadrement de la conservation des données par le droit européen ne saurait remettre en cause les exigences constitutionnelles tirées de la sauvegarde des intérêts fondamentaux de la nation, de la prévention des atteintes à l'ordre public - notamment à la sécurité des personnes et des biens, de la lutte contre le terrorisme, ainsi que de la recherche des auteurs d'infractions pénales. Il précise que *« ces exigences constitutionnelles, qui s'appliquent à des domaines relevant exclusivement ou partiellement de la compétence des États membres en vertu des traités constitutifs de l'Union, ne sauraient être regardées comme bénéficiant, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution »*. Se trouve ainsi concrétisée la jurisprudence relative aux principes inhérents à l'identité constitutionnelle de la France, donc sans équivalent en droit de l'Union[Note 13], le juge décidant de laisser le droit de l'Union inappliqué, dès lors qu'il s'agit d'assurer la garantie effective d'exigences constitutionnelles spécifiques, tenant ici à au maintien de l'ordre et à la sécurité nationale. On connaît bien l'inspiration de cette *« clause de sauvegarde constitutionnelle »*, prolongement de la jurisprudence d'autres cours européennes remontant aux années 1970[Note 14], et fondée sur l'équivalence des protections, permettant de faire prévaloir exceptionnellement le droit national « *tant que* » ou *« aussi longtemps que »* le droit européen s'avère moins protecteur de certaines exigences spécifiquement garanties à l'échelle nationale. On note cependant qu'ici, les exigences constitutionnelles qui prévalent, car jugées sans équivalent en droit de l'Union, ne sont pas tant spécifiques à l'ordre constitutionnel français que fondamentalement rattachées à la souveraineté de l'État français. La protection de la sécurité est en effet l'une des missions premières et fondamentales de l'État, et les conditions dans lesquelles il décide ou non d'exploiter les données numériques et de fixer les règles en la matière, relèvent de sa souveraineté. Le Conseil d'État souligne ici *« la responsabilité qui incombe à l'État en matière de sécurité et l'exigence d'efficacité que l'action étatique requiert dans ce domaine »*, ce qui justifie de conserver la maîtrise de la définition des exigences étatique en matière de sécurité[Note 15].

Quelles que soient les suites apportées à ce contentieux, notamment devant le Conseil constitutionnel[Note 16], il s'agit ici d'illustrer la façon dont la souveraineté numérique de l'État se concrétise ou se trouve contestée, s'agissant de la possibilité de décider des conditions de conservation des données et donc de fixer le point d'équilibre entre liberté et sécurité. Ici, ce n'est pas la technologie, ni les multinationales américaines, qui limitent la souveraineté de l'État, mais bien les conséquences de l'intégration européenne et l'extension progressive des champs de compétence de l'Union.

B. - La capacité de l'État à construire une solution nationale de *cloud souverain*

8. - Les États sont soucieux de protéger les données du risque de piratage, de pillage ou d'espionnage de la part d'entreprises, d'États ou d'entités malveillantes, en les conservant sur le territoire national, grâce à des solutions de *« cloud souverain »*[Note 17]. En France, l'État a développé une stratégie sur *« l'usage de l'informatique en nuage »*, visant à relocaliser le stockage des données sur des serveurs hébergés en France, voire en Europe. Ont été identifiés les établissements et services indispensables au fonctionnement de l'État (opérateurs d'importance vitale - OIV, opérateurs de services essentiels - OSE), dont les systèmes d'information font l'objet d'une sécurité renforcée[Note 18]. Les autorités ont soutenu le développement de projets français de *cloud* souverain, tel *Numergy* (société française de *cloud computing* fondée en 2012 par SFR et Bull) ou *Cloudwatt* (créé par Orange et Thalès) qui n'ont pas prospéré. Elles ont entrepris de protéger les données de l'Administration, y compris celles des collectivités territoriales, en tant qu'archives publiques au sens de l'article L. 211-4 du Code du patrimoine, aux fins de les faire bénéficier d'une protection particulière. Ces données ont été visées par un guide de bonnes pratiques, puis par une note du 5 avril 2016 relative au *cloud computing*[Note 19] émanant des services des ministères de l'Intérieur et du ministère de la Culture, adressée aux Préfets et aux collectivités locales, rappelant la nécessité, à peine d'illégalité, de choisir une solution de *« cloud souverain »*, c'est-à-dire garantissant que les données seront conservées dans des datacenters géographiquement situés en France et soumis au droit français. La note en question, qui a été abondamment commentée, définit la notion de *cloud* souverain comme *« un cloud dont les données sont entièrement stockées et traitées sur le territoire français »*. En annexe à la note, la notion est définie de façon plus précise et exigeante, comme *« un modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur les données par un service de cloud sont physiquement réalisés dans les limites du territoire national par une entité de droit français et en application des lois et normes françaises »*. La solution peut être privée ou publique, c'est bien le lieu géographique de stockage des données qui s'avère déterminant, dès lors qu'il conditionne le droit territorialement applicable, la confidentialité et la sécurité des données. Plus récemment, la Direction Interministérielle du Numérique (DINUM) a publié une circulaire réaffirmant l'interdiction formelle d'utiliser les clouds non souverains pour le travail collaboratif des agents publics[Note 20].

Or, précisément, le droit européen peut faire obstacle au développement des *cloud* souverains nationaux, perçus comme des obstacles à la libre circulation des données dans l'Union. C'est ainsi qu'un règlement UE 2018/1807 est venu interdire aux États de prévoir une obligation de stockage des données sur leur territoire, considérant que les restrictions géographiques, au sein de l'Union européenne, s'agissant de la conservation des données, sont des barrières qui doivent être éliminées[Note 21]. Certes cette réglementation ne concerne que les données non personnelles, et elle comprend une exception, pour les cas où la sécurité publique serait menacée. En application de l'article 51 du TFUE qui justifie des exceptions en matière de libre circulation pour les activités participant dans un État, *« même à titre occasionnel, à l'exercice de l'autorité publique »*, l'article 4 du règlement UE 2018/1807 prévoit que *« les exigences de localisation des données sont interdites, sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité »*. Reste que, sous réserve de cette exception d'application stricte, la réglementation européenne combat la généralisation du recours aux *cloud* souverains que les États travaillent à mettre en place. L'objectif est au contraire d'ouvrir la concurrence entre services de *cloud computing* au niveau européen pour les données privées et publiques non personnelles. Ainsi, la perspective d'un *cloud* souverain pour les archives publiques - assurant la conservation des données sur le territoire français - est directement visée, sauf à prouver qu'il en va de la sécurité publique[Note 22]. De même, le développement de solutions *« souveraines »* à l'échelle nationale pour le stockage des données de santé ou relatives aux défis environnementaux, parmi d'autres domaines stratégiques, se heurterait au droit européen.

En réponse, l'État français a dû adapter sa stratégie en distinguant trois niveaux de solutions de *cloud* selon la sensibilité des données (*cloud* interne/*cloud* intermédiaire/*cloud* externe), dans le cadre d'une approche *« multicloud »* visant à concilier des objectifs contradictoires : celui des États d'instaurer des clouds souverains définis par leur assise territoriale nationale, et celui de l'UE de supprimer les frontières nationales faisant obstacle à la libre circulation des données. Peut-être faut-il en conclure que la souveraineté numérique des États ne peut pas effectivement être affirmée à l'échelle nationale, et qu'il est temps de l'appréhender à l'échelle de l'Union, ce qui soulève des enjeux non moins complexes.

2. Vers une souveraineté numérique européenne en matière de conservation des données

9. - La conservation des données des citoyens, des administrations et des entreprises européennes par des prestataires européens, soumis au droit européen, est une garantie de leur protection. C'est tout l'enjeu de la construction d'une solution de *cloud* souverain européen. L'intérêt porté à cette stratégie a été accru du fait de la crise sanitaire récente, qui a entraîné dans les différents États membres la mobilisation de nouveaux outils numériques (application de *contact tracing*, *pass* sanitaire et vaccinal) fondés sur le traitement des données des utilisateurs, dans le domaine sensible de la santé, soulignant les conséquences de la dépendance persistante aux solutions technologiques américaines.

A. - Les enjeux du *cloud* souverain européen

10. - Compte tenu des difficultés de la justice américaine à obtenir les données hébergées par des entreprises américaines en dehors du territoire national[Note 23], les États-Unis ont adopté en 2018 le *« Cloud Act »* (*Clarifying Lawful Overseas Use of Data Act*), permettant aux forces de sécurité et aux agences de renseignements, sur réquisition d'un juge, d'obtenir des opérateurs et fournisseurs de services américains de *cloud computing* les données conservées dans leurs data-center, quelle que soit leur localisation physique, dans le cadre d'enquêtes judiciaires. Ce dispositif vient s'ajouter aux lois extra-territoriales déjà existantes aux États-Unis, visant à lutter contre le terrorisme ou la corruption. D'autres puissances, telles la Chine et la Russie, ont d'ailleurs adopté des dispositifs comparables.

Alors que des fuites de données vers les États-Unis ont été régulièrement révélées, le droit américain n'offre pas de garanties suffisantes, au regard des standards européens en la matière. En 2020, la Cour de justice de l'Union invalidait le *Privacy shield* entré en vigueur le 1er aout 2016[Note 24], au regard de

l'insuffisante protection des données personnelles des citoyens européens, actant le risque encouru pour la vie privée des utilisateurs d'un transfert des données aux entreprises américaines. Dès lors, le développement de solutions européennes de *cloud computing* sécurisée, fiable et compétitive est devenu une priorité Note 25, et dans un marché en forte progression, un vaste plan industriel et technologique a été mis en place.

Outre des investissements lourds et la mise en place d'un référentiel commun en matière de *cloud computing*, une démarche de labellisation à l'échelle européenne a été lancée, prolongeant les démarches nationales (exemple du label *SecNumcloud* français élaboré en 2016 par l'ANSSI) permettant de labelliser comme *« cloud de confiance »* les services de certains prestataires. En 2019, un projet de *cloud* européen Gaia X a été lancé sur la base d'une initiative franco-allemande, associant le leader européen du *cloud* installé en France, OVHcloud, et la filiale de services numériques de l'opérateur allemand Deutsche Telekom, T-Systems. Il s'agissait de créer une infrastructure de stockage de données efficace et compétitive, fiable et sécurisée garantissant l'interopérabilité, la réversibilité, la confiance et la transparence. Et ainsi de proposer une alternative crédible et performante, à destination des États et entreprises européennes, aux solutions de *cloud* proposées par Google, Microsoft ou Amazon. Plusieurs centaines d'entreprises ou d'établissements européens ont rejoint le projet (entreprises, hôpitaux, ministères et universités Note 26, y compris certaines filiales européennes d'entreprises étrangères (Huawei, Microsoft Belgique, Amazon europe, Palantir Technologies, alibaba...), ce qui tout à la fois augmente la performance des solutions techniques, et fragilise le projet. Chaque État membre de l'Union européenne intéressé est invité à organiser sur son territoire un *« hub »* permettant d'associer les partenaires intéressés, le French Gaia-X Hub ayant été lancé en mai 2021. Parmi d'autres initiatives, un processus de rapprochement industriel autour d'un projet important d'intérêt européen commun (PIIEC) sur les technologies Cloud a été lancé par la France et l'Allemagne fin 2021.

11. - Par ailleurs, à la suite d'un rapport de l'OCDE mettant en avant les pratiques antitrust de certains fournisseurs *cloud*, la législation sur les marchés numériques (*Digital Market Act - DMA*) adoptée en 2022 durcit les obligations et interdictions pesant sur les opérateurs du numérique pour garantir une concurrence loyale, et s'attaque ainsi aux géants du *cloud*. En effet, les services de *cloud* font partie des services de plateforme essentiels soumis à la nouvelle réglementation. La législation sur les marchés numériques devrait fixer des règles plus exigeantes à l'égard des plateformes, visant à les empêcher d'imposer des conditions inéquitables aux autres entreprises et aux utilisateurs. Ainsi, il sera interdit à un contrôleur d'accès de faire bénéficier les services et produits qu'il propose d'une visibilité ou d'un traitement plus favorable que les services et produits similaires proposés par des tiers sur sa plateforme. Après approbation le 18 juillet 2022 par le Conseil de l'Union, l'application de cette réglementation, prévue pour 2023, devrait permettre de rendre le marché du *cloud* plus équitable et compétitif, au bénéfice des entreprises européennes.

B. - La conservation des données de santé

12. - En mai 2022, la Commission européenne a publié un projet de règlement relatif à l'espace européen des données de santé (*European Health Data Space - EHDS*), visant à créer un cadre fiable, sécurisé, efficace et interopérable pour l'utilisation des données de santé au sein de l'Union et à relancer la politique de santé numérique de l'Union Note 27. Il s'agit à la fois de garantir aux citoyens la maîtrise de leurs données de santé, pour assurer la qualité de soins et la protection de leur vie privée, et aussi d'ouvrir les données plus largement à la recherche et aux acteurs de l'innovation. Un projet pilote est actuellement développé pour de premiers tests sur cinq cas d'usage, permettant de mesurer la faisabilité et le potentiel d'une réutilisation de données de plusieurs pays européens.

Définies par l'article 4-15 du RGPD comme *« les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de soins de santé, qui révèlent des informations sur l'état de santé de cette personne »*, les données de santé font l'objet d'une protection particulière. Leur traitement est en principe interdit par le RGPD, sous réserve d'exceptions limitativement énumérées (prévention de la santé publique, préservation des intérêts vitaux de la personne physique concernée, gestion des systèmes et services de santé ou de la protection sociale, consentement de la personne...) et d'obligations particulières imposées aux responsables de traitement.

Les enjeux du traitement des données de santé ont été démultipliés et révélés par la crise sanitaire Covid. La pandémie a touché tous les citoyens européens et a généré des politiques sanitaires d'urgence fondées sur de nouveaux outils numériques (création d'applications de *contact tracing*, élaboration des *pass* sanitaire et vaccinaux nationaux et européens). Elle a aussi ravivé la concurrence des laboratoires de recherche à travers le monde, rivalisant dans le traitement des données disponibles pour mettre au point des politiques de préventions, des traitements curatifs et des vaccins.

Les conditions de recueil, de stockage, d'exploitation des données de santé soulèvent des enjeux politiques, juridiques et économiques majeurs, d'autant que l'urgence de la situation n'a pas permis d'adapter la réglementation ou d'établir les conditions de la confiance et d'une concurrence loyale. Au contraire la pandémie a accentué l'emprise croissante des procédés de surveillance généralisée des populations et amplifié les intérêts économiques en jeu.

Tandis que l'Union européenne s'attache à créer un espace sécurisé des données de santé, les contentieux se sont multipliés à l'échelle nationale, au regard de la dépendance des États vis-à-vis des solutions techniques proposées par les multinationales américaines. Il en ressort la difficulté à établir la confiance lorsqu'il est fait appel aux filiales européennes de multinationales américaines, s'agissant d'assurer la sécurité des données personnelles de santé, dans le cadre des solutions techniques de stockage qu'elles proposent. En France, le lancement en 2019 de la plateforme de collecte et d'analyse des données de santé (*Health Data Hub)* a occasionné des actions en justice, en raison du recours aux services de Microsoft Azure, et alors même que les données étaient localisées en Europe, et surtout après l'invalidation du *Privacy shield* par la CJUE qui a discrédité le processus d'autocertification dont se prévalait la multinationale américaine en matière de protection des données. Le Conseil d'État a reconnu l'existence d'un risque de transfert de données vers les États-Unis, notamment lors d'opérations de gestion et de maintenance, et préconisé le développement de solutions souveraines, sans pour autant suspendre la plateforme existante, compte tenu du contexte de pandémie Note 28.

13. - Par ailleurs, pour la mise en place d'un outil de *contact tracing* (*StopCovid* puis *TousAntiCovid)*, la France a refusé la solution technologique proposée par Apple et Google dite *« Exposure notification »*, pour promouvoir une solution plus *« souveraine »*, dont le lancement a mobilisé des partenaires publics et privés français (INRIA, ANSSI, Dassault, Capgemini..), et qui a permis un stockage des données sur le territoire national, même si certaines phases de développement ont nécessité le recours à des API Note 29 d'entreprises américaines (Google, Akamaï technologies). Enfin, la gestion de la campagne vaccinale a accentué la prise de conscience, lorsqu'il est apparu que les entreprises françaises ou européennes mobilisées pour la gestion des prises de rendez-vous restaient dépendantes, à la marge, des géants américains, telle l'entreprise Doctolib qui s'appuie sur les solutions techniques d'AWS, filiale d'Amazon. Le Conseil d'État,

saisi en référé, a ici considéré qu'il n'y avait pas d'atteinte grave et manifestement illégale au droit au respect de la vie privée et à la protection des données personnelles[Note 30] dès lors que la plateforme Doctolib n'a pas à connaître de l'état de santé de ses utilisateurs, ne conserve pas les données au-delà de 3 mois et garantit le chiffrement des données.

14. - Comme la France, les États membres de l'Union européenne ont été confrontés à un arbitrage entre l'efficacité de la gestion de la crise sanitaire et le risque de voir les données de santé de leurs populations captées et exploitées par des acteurs étrangers, qui se sont avérés être les seuls suffisamment performants. Les contextes d'urgence sanitaire et terroriste ont accéléré la prise de conscience : la conservation et l'exploitation des données doivent être encadrées de façon à assurer à la fois la garantie des droits des citoyens européens, l'efficacité des politiques publiques de protection des populations (sécurité, santé), et la compétitivité des entreprises européennes. L'adaptation en cours de la réglementation et la relance des politiques industrielles valorisant des solutions techniques fiables, maîtrisées par des opérateurs soumis au droit européen, devraient contribuer utilement à cet objectif.

Mots clés : Numérique. - Donnée.

Mots clés : Numérique. - Souveraineté.

Mots clés : Numérique. - Sécurité.

Egalement dans ce dossier :

Note 1 *Comprendre la souveraineté numérique : Cahiers français, n° 415, mai-juin 2020, 23 juin 2020. - A. Blandin-Obernesser (dir.), Droits et souveraineté numérique en Europe : Bruylant, 2016. - P. Türk et C. Vallar (dir.), La souveraineté numérique, le concept, les enjeux : Mare & Martin, 2018. - C. Castets-Renard, L. Rass-Masson, V. Ndior (dir.), Enjeux internationaux des activités numériques, Entre logique territoriale des États et puissance des acteurs privés : Larcier, 2020.*

Note 2 *V. les écrits de J. Bodin, L. Le Fur, puis R. Carré de Malberg, parmi les théoriciens de l'État et de la souveraineté.*

Note 3 *Déclaration d'indépendance du Cyberespace, J. Perry Barlow, 1996, Davos.*

Note 4 *SMSI de 2003 à Genève et de 2005 à Tunis, Internet Governance Forum annuels (Bali 2013, Paris 2018), Conf. mondiale de l'UIT en 2012, NETmundial de Sao Paulo en 2014, etc.*

Note 5 *BVerfGE 65,1, Volkszählung, 15 déc. 1983. - BVerfG 27,1, Mikrozensus, Beschluss v. 16 juill. 1969. - BVerfG 34,238, Tonband 31 janv. 1973 - 2 BvR 454 /71. - CEDH, 27 juin 2017, n° 931/13, Satakunnan Markkinaporssi oy et Satamedia oy c/ Finlande, § 137. - CEDH, 24 avr. 2018, n° 62357/14, Benedik c/ Slovénie , § 103.*

Note 6 *B. Bertrand, La souveraineté numérique européenne : une « pensée en acte » ? : RTD eur. 2021, p. 249.*

Note 7 *Rapp. AN n° 4082, 2016, d'information de la mission d'information constituée le 3 février 2016 sur l'extraterritorialité de la législation américaine.*

Note 8 *PE et Cons. règl. (UE) 2018/1807, 14 nov. 2018, établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne (free flow of data).*

Note 9 *V.-L. Benabou, Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? : RTD eur. 2021, p. 279.*

Note 10 *BVerfG 5 mai 20202 BvR 859/15, 2 BvR 980/16, 2 BvR 2006/15, 2 BvR 1651/15. - Tribunal constitutionnel polonais, 7 oct. 2021. - R Mehdi, Heurs et malheurs de l'État de droit, l'Union européenne au défi d'une crise essentielle : Rev. UE 2022, p. 240. - C. Blumann, Quelques enseignements de l'arrêt du Bundesverfassungsgericht du 5 mai 2020 sur les fondamentaux du droit de l'Union européenne : RTD eur. 2020, p. 889.*

Note 11 *CJUE, 21 déc. 2016, aff. C-203/15, Télé2 Sverige, confirmée par CJUE, 2 oct. 2018, aff. C-207/16, Ministerio Fiscal, et précisée, sur renvoi préjudiciel, par CJUE, 6 oct. 2020, aff. C623-17, Privacy international et, CJUE, 6 oct. 2020, aff. C-511-18, La Quadrature du net. - A. Deroudille, L'exploitation généralisée et indifférenciée des données de connexion en question : Rev. UE, n° 659, juin 2022 p. 332. - J. Sirinelli, La protection des données de connexion par la Cour de justice : cartographie d'une jurisprudence européenne inédite : RTD eur. 2021, p. 313.*

Note 12 *CE, ass., 21 avr. 2021, n° 393099, French data network : Lebon ; JCP A 2021, 2223 ; AJDA 2021, p. 828 ; D. 2021, p. 797. - A. Iliopoulou-Penot, La conservation généralisée des données de connexion validée, le droit au désaccord avec la Cour de justice revendiqué : JCP G 2021, n° 24, p. 659.*

Note 13 *Cons. const., 19 juin 2004, n° 2004-496 DC, Confiance dans l'économique numérique ; Cons. const., 27 juillet 2006, n° 2006-540 DC, Droits d'auteurs et droits voisins dans la société de l'information ; Cons. const., 19 juin 2008, n° 2008-564 DC, OGM. ;CE, 8 févr. 2007, n° 287110, Arcelor ; JCP A 2007, 2081, obs. G. Drago ; Procédures 2007, comm. 96, obs. S. Deygas ; Cons. Const. 15 octobre 2021, n° 2021-940 QPC Société Air France.*

Note 14 *V. jurisprudence « So lange » de la Cour constitutionnelle allemande des 18 octobre 1974, 22 octobre 1986 et 7 juin 2000 (BVerfGE 37, 271 29/05/1974 ; Re Wünsche Handelsgesellschaft BVerfGE 73, 339 ; BVerfGE 89, 155 aff 12/10/1993 ; et BVerfGE, 7 juin 2000 Bananenmarktordnung). - V. aussi les arrêts de la Cour constitutionnelle italienne n° 183 du 27 décembre 1973 Frontini et Pozzani, Granital en 1984 et Spa Fradg de 1989 ; ou la décision du Tribunal constitutionnel espagnol du 13 décembre 2004.*

Note 15 *L. Azoulai, D. Ritleng, L'État, c'est moi : le Conseil d'État, la sécurité et la conservation des données : RTD eur. 2021, p. 353, 368.*

Note 16 *Dans sa décision n° 2021-976/977 QPC du 25 février 2022 (conservation des données à caractère personnel pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales), le Conseil constitutionnel censure comme portant une atteinte disproportionnée au droit au respect de la*

vie privée des dispositions législatives concernant la conservation des données de connexion, dans leur version antérieure à la loi n° 2021-998 du 30 juillet 2021. - C. Crichton, Inconstitutionnalité de la conservation généralisée et indifférenciée de métadonnées : Dalloz IP 2022, p. 118.

Note 17 *B. Delmas-Linel et C. Mutz, Le cloud computing à l'épreuve des souverainetés nationales : Faut-il avoir peur du USA Patriot Act ? : RDLI, 1er avr. 2013, n° 90. - F. Plénacoste et E. Daoud, Cloud Act : des inquiétudes légitimes : Dalloz IP, 2018, p. 680. - B. Fauvarque-Cosson, C. Zolynski (dir), Le cloud computing. L'informatique en nuage, vol. 22, 2014, 157 p.*

Note 18 *L. n° 2013-1168, 18 déc. 2013, relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.*

Note 19 *Note d'information n° DGP/SIAF/2016/006, 5 avr. 2016, relative à l'informatique en nuage (cloud computing).*

Note 20 La circulaire du 15 septembre 2021 implique le développement de solutions souveraines, pour une « *digital workplace* » sécurisée, dès lors que la suite logicielle Microsoft 365 a été déclarée par la DINUM non conforme à la doctrine du « *Cloud au Centre* ».

Note 21 *V.-L. Benabou, Une cinquième liberté de circulation numérique ? Est-ce possible ? Est-ce utile ? : RTD eur. 2021, p. 279.*

Note 22 *J. Mouchette, Haro sur les obligations de localisation des données non personnelles : Dalloz IP, 2020, p. 401. - V. notion de « raison impérative justifiant une restriction » à la libre prestation des services ou à la libre circulation, CJUE, Cour, 26 févr. 1991, aff. C-154/89, Commission c/ France.*

Note 23 *United States v. Microsoft Corp. 584 U.S., 138 S. Ct. 1186 (2018)*

Note 24 *CJUE, 16 juill. 2020, Schrems II, préc.*

Note 25 *E. Le Quellenec, L'émergence d'un cloud souverain européen : Revue Lamy, droit de l'immatériel, 1er août 2020, n° 173.*

Note 26 *Siemens, Orange, Bosch, Thalès, airbus, Engie, VW, la SNCF, BNP Paribas, Crédit agricole, MEDEF, ministère de l'Éducation nationale, ENS Paris-Saclay, université d'Amsterdam, hôpital principal de Barcelone, etc.*

Note 27 *Proposal for a regulation - The European Health Data Space : COM (2022) 197/2.*

Note 28 *CE, ord. réf., 19 juin 2020, n° 440916, Heath data hub. - CJUE, 16 juill. 2020, aff. C-311/18, Data Protection Commissioner c/ Facebook Ireland Ltd, Maximillian Schrems. - CE, 13 oct. 2020, n° 444937. - L. Cluzel-Métayer, L'hébergement de la plateforme des données de santé par Microsoft : une validation sous surveillance : AJDA 2021, p. 741.*

Note 29 Application Programming Interface ou interface de programmation d'application, solution informatique qui permet à des applications de communiquer entre elles et de s'échanger mutuellement des services.

Note 30 *CE, 12 mars 2021, n° 450163, InterHop. - B. Bertrand et J. Sirinelli, L'affaire Doctolib devant le Conseil d'État : le secret de la Licorne : Dalloz IP 2021, p. 518.*