Jeudi 11 mai 2023

- Présidence de M. Jean-François Rapin, président -

La réunion est ouverte à 9 h 10.

Marché intérieur, économie, finances, fiscalité - Proposition de règlement européen sur les données (« Data Act ») - Accessibilité et usage des données - Examen de la proposition de résolution européenne et de l'avis politique

M. Jean-François Rapin, président. - Mes chers collègues, les technologies numériques tiennent une place désormais centrale dans nos vies quotidiennes et transforment profondément l'économie et la société. Leur développement ouvre de formidables perspectives, mais favorise également des comportements préjudiciables. Il crée en outre des tensions, dans un univers interconnecté mondialisé, dominé par de très grands acteurs, le plus souvent américains ou chinois.

L'Union européenne (UE) s'attelle à construire une régulation du numérique dans le marché intérieur, pour protéger ses citoyens et ses valeurs et pour assurer le respect des règles de concurrence. Elle a ainsi récemment adopté plusieurs législations importantes, dont le règlement relatif aux marchés contestables et équitables dans le secteur numérique. Cette législation sur les marchés numériques, le *Digital Markets Act* (DMA), vise à rétablir la concurrence mise à mal sur le marché intérieur par les pratiques abusives des grandes plateformes qualifiées de « contrôleurs d'accès », en encadrant leurs comportements de domination et d'éviction.

Afin que ne soit pas praticable en ligne ce qui est interdit hors ligne, l'Union européenne a également adopté une législation sur les services numériques, le *Digital Services Act* (DSA), qui encadre les activités des plateformes afin de lutter contre la haine en ligne, la manipulation, la désinformation ou la vente de produits contrefaits.

Nous avons déjà eu l'occasion d'étudier ces textes européens et d'adopter des résolutions pour en renforcer la portée et l'efficacité. D'ailleurs, le Sénat examinera bientôt le projet de loi déposé hier par le Gouvernement pour assurer leur transposition en droit national.

En complément du DMA et du DSA, la Commission européenne a aussi présenté, le 19 février 2020, deux stratégies européennes : l'une dédiée à l'intelligence artificielle (IA), l'autre aux données. Dernièrement, en mars, c'est l'intelligence artificielle qui a mobilisé notre commission, afin de contribuer à ce que son déploiement sur notre continent respecte les valeurs européennes.

L'objet de notre réunion de ce jour est d'aborder l'autre volet : le sujet des données, souvent qualifiées d'« or noir » à l'ère numérique. Mme Blatrix Contat, Mme Morin-Desailly et M. Gattolin vont nous présenter la stratégie européenne en la matière et, plus spécialement, leur rapport sur la proposition de règlement européen sur les données, le *Data Act*.

Mme Florence Blatrix Contat, rapporteure. - Nous allons effectivement vous présenter aujourd'hui le volet législatif de la stratégie européenne pour les données visant à réduire les obstacles de différentes natures auxquels se heurte la construction en cours du partage des données au sein de l'UE.

La Commission a identifié un certain nombre de barrières qui empêchent la libre circulation effective des données au sein de l'Union, au premier rang desquelles la faible confiance dans le partage des données. Elle a également constaté que des pratiques de verrouillage empêchent les personnes, physiques ou morales, d'exercer pleinement leurs droits à accéder aux données générées par l'utilisation d'objets connectés et de services numériques liés, à en suivre l'utilisation et à en permettre la réutilisation dans les écosystèmes numériques. En effet, des déséquilibres en termes de pouvoir de marché permettent aux contrôleurs d'accès de concentrer les données et d'imposer unilatéralement des conditions d'accès et d'utilisation qui en empêchent le partage.

La Commission a en outre constaté que la réutilisation des données se heurte à des obstacles techniques significatifs en raison de difficultés d'interopérabilité et de qualité des données, en l'absence de normes impératives en la matière. Elle a par ailleurs identifié des problématiques liées à la disponibilité des données, en particulier des données du secteur public, et à la collecte de données dans l'intérêt commun.

Enfin, elle n'a pu que constater que la souveraineté européenne sur les données n'est pas assurée. En raison du rôle marginal des fournisseurs européens de *cloud*, les fournisseurs étrangers opérant dans l'UE jouent un rôle prédominant, alors même qu'ils sont soumis à la législation applicable aux États tiers, avec les risques en résultant en matière de protection des données et de cybersécurité.

Pour remédier à ces insuffisances, la Commission a publié une stratégie européenne pour les données, destinée à mettre en place un espace européen des données, dont les règles communes et les mécanismes d'application doivent tout à la fois garantir les points suivants : la circulation des données à l'intérieur du marché unique et entre les secteurs, dans le respect des règles et valeurs européennes, en particulier la protection des données à caractère personnel - fil rouge du texte - ; une concurrence efficace sur le marché intérieur, en prévoyant des règles d'accès et d'utilisation des données équitables, pratiques et fiables ; des mécanismes de gouvernance des données clairs et fiables ; enfin, une approche ouverte des flux internationaux de données, mais affirmée et fondée sur les valeurs européennes.

Les actions proposées par la Commission reposent sur quatre piliers : des mesures horizontales trans-sectorielles pour l'accès aux données et leur utilisation ; des investissements dans les données et le renforcement des capacités et des infrastructures européennes pour l'hébergement, le traitement et l'utilisation des données ainsi que leur interopérabilité ; le développement des compétences en matière numérique ; le développement d'espaces européens communs des données dans des secteurs économiques stratégiques et des domaines d'intérêt public, en particulier les données relatives au pacte vert, en matière de santé, de mobilité, ou encore d'énergie.

Après le récent règlement sur la gouvernance des données, dit *Data Governance Act*, qui est destiné à faciliter la réutilisation des données du secteur public, et qui sera applicable à compter du 24 septembre prochain, la proposition de règlement sur les données, dite *Data Act*, sur laquelle nous nous penchons aujourd'hui, s'inscrit dans le premier pilier. En effet, elle définit un cadre juridique et technique horizontal pour permettre une répartition

plus équitable de la valeur des données industrielles entre les acteurs de l'économie des données.

Les données concernées sont les données produites par l'utilisation d'objets connectés et de services liés. Point important : il s'agit donc de données primaires, non traitées, ce qui devrait d'ailleurs être plus clairement précisé dans le texte, comme nous le préconisons dans la proposition de résolution que nous vous soumettrons. Le volume de ces données connaît depuis quelques années un développement exponentiel en raison du nombre croissant d'objets connectés : 8 milliards d'objets en 2019, 13,8 milliards attendus en 2024. Or ces données, qualifiées d'industrielles, sont peu exploitées en Europe. Lors de son discours de 2020 sur l'état de l'Union, la présidente de la Commission européenne a ainsi précisé que 80 % d'entre elles ne sont pas utilisées. D'où le grand intérêt de ce texte.

M. André Gattolin, rapporteur. - Le *Data Act* prévoit un droit d'accès et de partage encadré. Il reconnaît aux utilisateurs des objets connectés des droits sur les données produites par leur utilisation de ces objets et de services liés. Il fixe des règles harmonisées en matière d'accès, d'utilisation et de partage de ces données entre entreprises et consommateurs et interentreprises. Enfin, il définit les obligations des détenteurs des données tenus de rendre des données disponibles.

Nous avons donc affaire à trois protagonistes : l'utilisateur de l'objet connecté et de services liés, qui peut être une personne physique - un consommateur -, ou une personne morale - une entreprise - ; le détenteur des données produites par cet objet, qui en est généralement le fabricant ; le destinataire des données, entreprise tierce désignée par l'utilisateur en raison de son activité, afin qu'il puisse utiliser les données à des fins précises, notamment de réparation de l'objet connecté.

L'utilisateur de l'objet connecté se voit reconnaître un double droit sur les données générées par son utilisation de l'objet connecté et des services liés : un droit d'accès gratuit et un droit d'utilisation, y compris pour les partager avec des tiers.

La proposition de règlement précise la portée du droit d'accès de l'utilisateur aux données, y compris en termes de qualité des données. Elle prévoit des mesures pour en faciliter la mise en oeuvre, en particulier l'obligation de prévoir l'accès aux données dès la conception, dit *by design*, et d'assurer la protection de la confidentialité et de la sécurité des données.

Le partage des données avec un tiers désigné par l'utilisateur est également encadré : les données transférées doivent présenter un niveau de qualité identique ; une compensation raisonnable des coûts de mise à disposition peut être facturée ; l'utilisation des données est limitée aux fins et conditions convenues avec l'utilisateur, pour la fourniture d'un service ; profilage et manipulation des données sont prohibés. Un dispositif de règlement des conflits est prévu en cas de litige.

Enfin, il est proposé de corriger les déséquilibres contractuels constatés en rééquilibrant le pouvoir de négociation des micro, petites et moyennes entreprises dans les contrats de partage de données et en écartant les grandes plateformes du bénéfice de ce partage.

Plusieurs points doivent être précisés. Nous proposons tout d'abord d'affirmer fermement la primauté des règles de protection des données à caractère personnel, en particulier du règlement général sur la protection des données (RGPD) et de la directive sur la protection de la vie privée dans le secteur des communications électroniques. De telles données à caractère personnel peuvent en effet être mêlées aux données dont nous parlons.

Une attention toute particulière doit en outre être portée aux situations dans lesquelles les données sont celles non pas de l'utilisateur titulaire, mais, par exemple, d'un salarié ou d'un membre tiers du foyer.

Deuxième point d'attention : il faut assurer l'effectivité des droits des utilisateurs sur les données. Cela suppose en particulier que le format des données soit compréhensible, structuré, habituel et lisible par la machine et que les métadonnées nécessaires à leur interprétation soient communiquées. Nous proposons de rendre obligatoire le respect de ces exigences techniques.

Dans un souci d'équilibre de la relation contractuelle entre l'utilisateur et le détenteur des données, nous préconisons par ailleurs que soient identifiées des clauses abusives afin de les priver d'effet.

S'agissant du partage des données avec des tiers, il nous semble pertinent de maintenir l'exclusion proposée des grandes plateformes dites « contrôleurs d'accès » en raison de leur pouvoir de marché excessif. Je signale toutefois que ce point est contesté par certaines entreprises, au nom de la cohérence du fonctionnement des chaînes de valeur.

Afin d'équilibrer les accords de partage conclus entre le détenteur des données et le tiers utilisateur, il est prévu de rendre inopposables un ensemble de clauses considérées comme abusives, ce qui, là encore, nous paraît pertinent. La compensation des coûts de mise à disposition des données devrait toutefois être mieux encadrée.

Venons-en maintenant à un sujet particulièrement sensible : la protection des secrets d'affaires. Qui dit protection ne dit pas refus de communiquer des données pour ce motif - le texte ne l'autorise pas -, mais interdiction de les utiliser à des fins concurrentielles - ce qui est prévu -, et mise en place de mesures de protection, en particulier contractuelles, ce qui est également prévu. Encore faudrait-il que ces mesures n'excèdent pas les besoins légitimes d'assurer cette protection.

Nous vous proposons malgré tout de considérer que, dans certains cas exceptionnels, la protection de secrets d'affaires puisse justifier un refus de transmettre les données. Notre attention a ainsi été attirée sur la possibilité de déduire de données brutes des éléments clés sur les dispositifs de sécurité inclus dans le produit connecté - c'est notamment le cas dans le domaine de l'aviation. Pour justifier un refus en pareil cas, le détenteur des données devrait démontrer que leur divulgation est de nature à avoir des conséquences dommageables graves, y compris au regard de la sécurité.

J'en viens à un point particulier : l'accès d'autorités publiques nationales et européennes à des données en cas d'urgence publique. Un chapitre du *Data Act* est consacré à la mise à disposition de ces autorités de données détenues par le secteur privé, en cas de besoin exceptionnel.

Trois situations sont considérées comme constitutives d'un tel besoin exceptionnel : lorsque les données sont nécessaires pour réagir à une urgence publique ; lorsqu'elles sont nécessaires pour prévenir une telle urgence ou contribuer au rétablissement à la suite d'une telle urgence ; lorsque l'absence de données disponibles empêche l'organisme de s'acquitter d'une mission d'intérêt public prévue par la loi et qu'il ne lui a pas été possible d'obtenir ces données par d'autres voies.

Je ferai plusieurs observations. Tout d'abord, l'urgence publique est définie comme une situation exceptionnelle qui a des conséquences négatives

pour la population de l'Union, d'un État membre ou d'une partie de celui-ci, entraînant un risque de répercussions graves et durables sur les conditions de vie, la stabilité économique ou la situation d'actifs économiques. Nous vous proposons de demander que la nature de l'urgence soit précisée en indiquant expressément quelles sont les circonstances visées : santé, catastrophe, cyberattaque, par exemple. Les conséquences de la situation exceptionnelle justifiant l'exercice de ce droit d'utilisation des données doivent également être précisées. Il est ainsi préférable de parler d'atteinte à la stabilité financière ou à des actifs économiques majeurs, plutôt que de faire référence à la « stabilité économique » ou la « situation d'actifs économiques ».

La troisième situation visée par la proposition de règlement - l'absence de données disponibles empêchant l'organisme de s'acquitter d'une mission d'intérêt public - est recevable, mais il nous semble qu'elle doit être plus précisément encadrée, qu'il s'agisse de la durée et de la portée de la mise à disposition des données, de la démonstration de l'impossibilité de trouver ces données et de l'obligation de ne les utiliser que pour les seules finalités de la demande, dans le strict respect des droits et libertés des personnes.

Mme Catherine Morin-Desailly, rapporteure. - Le second objectif du texte est de permettre une mobilité effective et sécurisée des données.

Trois dimensions de cette mobilité sont ainsi traitées : le changement de fournisseur de services de traitement des données, autrement dit de *cloud* ; la définition des conditions techniques permettant cette mobilité, autrement dit la portabilité et l'interopérabilité des données ; enfin la sécurisation des flux internationaux de données.

S'agissant de la mise en oeuvre du droit de changer de fournisseur de *cloud*, la proposition de règlement s'attaque à une vraie difficulté. Le marché de l'informatique en nuage est fortement concentré : 72 % du marché européen est ainsi contrôlé par trois fournisseurs américains, Microsoft Azure, AWS et Google Cloud, ce qui laisse peu de place aux fournisseurs européens, dont la part relative tend à régresser rapidement. La raison en est un fort lobbying de ces trois acteurs et un déficit de politique industrielle volontariste pour accompagner le développement du *cloud* européen.

Ces acteurs dominants, dits *hyperscalers*, ont recours à des pratiques de verrouillage qui empêchent les utilisateurs de changer de fournisseurs et, par voie de conséquence, le développement de concurrents. Ces pratiques sont techniques, juridiques et financières, en particulier le recours à des formats propriétaires et la facturation de frais de sorties très élevés. Les personnes auditionnées ont particulièrement insisté sur ce point.

On constate également des abus de position de marché. Ces très grands acteurs convertissent ainsi leur position forte au sein d'une couche du *cloud* - câbles, *data centers,* serveurs ou logiciels de traitement - en une position dominante au sein d'autres couches, par exemple en recourant à la vente liée, ou en appliquant des mesures de représailles. Vous trouverez des détails à ce sujet dans notre rapport d'information.

Pour supprimer les obstacles commerciaux, techniques, contractuels et organisationnels au changement de fournisseur de services de traitements de données, le chapitre VI de la proposition de règlement soumet le fournisseur initial de services de traitement des données à un ensemble d'obligations et met en place un cadre de préparation et d'accompagnement du changement. Enfin, il prévoit une interdiction progressive de facturer des frais de changement à horizon de trois ans.

Les mesures proposées permettront aux clients de pouvoir changer de fournisseur de services de traitement des données lorsqu'ils le souhaitent. Certains compléments pourraient toutefois y être utilement apportés, afin que le client soit pleinement informé en la matière, y compris avant l'acceptation de l'offre de service. Il devrait également être précisément informé sur les étapes du processus de migration et les diligences à mettre en oeuvre.

Par ailleurs, il conviendrait d'interdire au fournisseur de services de traitement des données d'empêcher un client de changer de fournisseur au motif qu'il aurait bénéficié d'une phase d'utilisation gratuite de ses services. Peut-on même admettre ces pratiques de gratuité, forme de *dumping* ? Telle est la question que nous nous sommes aussi posée.

Quant au délai de mise en oeuvre de la suppression des frais de sortie - trois ans -, il nous paraît difficilement acceptable, sauf à anéantir toutes velléités concurrentielles sur le marché intérieur.

Venons-en maintenant à l'interopérabilité. La combinaison de données provenant de différentes sources à l'intérieur des secteurs et entre les secteurs ne peut être mise en oeuvre si les espaces de données ne sont pas interopérables. Le frein majeur à une interopérabilité optimale est l'utilisation de formats dits propriétaires et l'absence de protocoles de communication.

La proposition de règlement impose aux exploitants - d'espaces de données, de mécanismes de partage de données et des services dans ces domaines - un ensemble d'exigences essentielles en matière d'interopérabilité des données et d'interopérabilité des services de traitement des données, ainsi qu'en matière de contrats intelligents pour le partage des données, autant de domaines dans lesquels il n'existe pas de normes harmonisées, ou de normes suffisantes en la matière. Il est prévu que des normes harmonisées soient publiées. Sans doute serait-il utile de préciser d'ores et déjà l'objet de ces normes et leur processus d'élaboration, en particulier le rôle des parties prenantes.

J'en viens à la sécurité des données en cas de transferts internationaux, dernier point crucial traité par la proposition de règlement, en raison de l'application extraterritoriale de leurs lois par des États tiers sur des données européennes, en méconnaissance du droit européen ou du droit national, en particulier en matière de protection des droits fondamentaux de la personne, des intérêts fondamentaux d'un État membre pour des raisons tenant à la sécurité ou la défense nationales, aux secrets d'affaires ou aux droits de propriété intellectuelle.

En l'absence d'accord international - le régime de transferts de données entre l'Union européenne et les États-Unis, dit *Privacy Shield*, a été invalidé - , la proposition de règlement prévoit des garanties spécifiques de protection des données, et soumet les fournisseurs de services de traitement de données à l'obligation de prendre « toutes les mesures techniques, juridiques et organisationnelles raisonnables » afin d'empêcher le transfert hors du territoire européen de données à caractère non personnel qui y sont détenues ou l'accès d'un État tiers à celles-ci.

Il s'agit indiscutablement d'une démarche positive. Mais rappelons que, étant donné la législation américaine, incluant le *Foreign Intelligence Surveillance Act* (FISA) et le *Cloud Act*, nous aurons beau voter toutes les législations possibles, dès que nous aurons affaire à un fournisseur de la *Big Tech*, le transfert des données sera rendu obligatoire. Il nous semble donc tout aussi indispensable d'établir une liste de données sensibles et de données dont la divulgation est susceptible de porter atteinte à la sécurité nationale que de doter l'Europe d'infrastructures souveraines sécurisées, qui ne soient pas contrôlées par des capitaux étrangers.

J'en viens au dernier sujet : la supervision de la mise en oeuvre du règlement. Elle est organisée au niveau national et doit être confiée à des autorités dotées de pouvoirs de surveillance, d'injonction, astreinte et de sanctions. Ces pouvoirs pourraient être utilement complétés par la possibilité d'imposer des remèdes aux professionnels défaillants. Par ailleurs, dès lors que des données à caractère personnel sont en cause, une attention particulière devra être portée à l'articulation entre ces autorités chargées de superviser l'application du règlement sur les données et celles qui sont en charge de la protection de ces données personnelles. Enfin, pour renforcer l'efficacité de la coopération intra-européenne en matière de données, qui est nécessaire à une mise en oeuvre efficace et coordonnée du règlement, la mise en place d'une structure de coordination, réunissant des représentants des autorités nationales de contrôle concernées nous paraît s'imposer.

Voilà l'ensemble de nos préconisations, rassemblées dans la proposition de résolution européenne que nous vous soumettons.

Pour conclure, je précise que, dans le projet de loi sur le numérique que le Gouvernement vient de déposer sur le bureau du Sénat à l'initiative du ministre Jean-Noël Barrot, est présente par anticipation la question des fournisseurs de services de traitement de données, notamment de l'interopérabilité et du transfert des données.

M. Jean-François Rapin, président. - Je vous remercie pour votre grande expertise, sur des sujets certes austères, mais dont le retentissement sera considérable. La transposition à venir que constitue le texte du ministre Barrot devra s'inspirer de vos travaux, dont j'ai rappelé l'importance.

M. André Reichardt. - La proposition de règlement est essentielle, et votre proposition de résolution l'est tout autant. J'y souscris pleinement.

Cependant, l'alinéa 29 ne devrait-il pas plutôt indiquer que le service de communication électronique est exclu du champ d'application de la proposition de règlement ? Cela serait plus clair et plus simple que la rédaction proposée.

Par ailleurs, vous me semblez trop prudents, à l'alinéa 46, sur le renforcement de la protection des droits de l'utilisateur. Ne devrions-nous pas préconiser l'interdiction de certaines clauses, plutôt que demander à examiner l'opportunité d'une telle interdiction ? Selon moi, les clauses abusives devraient être considérées comme non écrites.

Mme Catherine Morin-Desailly, rapporteure. - Nous avons privilégié cette formulation parce qu'il faut d'abord identifier de telles clauses, ce qui reste à faire.

M. André Reichardt. - Enfin, dès lors qu'on autorise les autorités publiques nationales et européennes à accéder aux données en cas d'urgence, il faut préciser la nature de celle-ci. Ainsi, à l'alinéa 68, ne faudrait-il pas définir des éléments quantitatifs, s'agissant de la temporalité de l'urgence et de ses conséquences ? En particulier, à quoi renvoie la notion d'« actifs économiques majeurs » ? Il faut encadrer au maximum l'accès à ces données. L'urgence doit être objective.

M. Jean-François Rapin, président. - Il y a l'urgence liée au numérique, mais aussi celle qui relève d'un état de catastrophe.

M. Didier Marie. - En cas de crise majeure, l'urgence est appréciée par l'État membre et pas par la Commission européenne. La proposition de règlement est une simple couche d'harmonisation. Mais la définition de l'urgence n'est pas harmonisée au niveau européen.

Mme Florence Blatrix Contat, rapporteure. - L'urgence est déjà encadrée par la proposition de règlement et les compléments que nous proposons d'y apporter. Peut-on aller au-delà ? Par définition, on ne peut pas prévoir tous les cas d'urgence.

M. André Gattolin, rapporteur. - On n'aurait pas imaginé la pandémie avant 2019…

Mme Pascale Gruny. - N'oublions pas l'effet sur la recherche d'un trop grand verrouillage de l'accès aux données.

M. André Reichardt. - Cela étant, je salue votre travail, soutenu et détaillé. Il est d'autant plus nécessaire au regard du contenu du projet de loi visant à sécuriser et réguler l'espace numérique présenté hier en conseil des ministres.

M. Jean-François Rapin, président. - Nous ne devons pas prêter le flanc aux critiques sur le respect de la subsidiarité. À chaque État membre de définir l'état d'urgence. Pouvons-nous demander plus d'harmonisation en ce domaine ? Je n'en suis pas certain.

M. André Reichardt. - Ce n'est pas ce que je propose : il s'agit plutôt de définir un cadre temporel de l'urgence, quitte à avoir des variantes de délais au sein de ce cadre, d'un État à l'autre.

M. Jean-François Rapin, président. - À qui s'en remettre, alors, pour une telle définition ? Au Conseil ?

Mme Catherine Morin-Desailly, rapporteure. - J'observe que la notion d'urgence présentait les mêmes difficultés de définition pour l'instrument d'urgence pour le marché intérieur. Peut-être y a-t-il d'ailleurs une articulation à trouver avec ce texte, ainsi qu'avec tous les textes sectoriels prévoyant des situations d'urgence, comme en matière de santé. Je ne suis pas certaine qu'on puisse aller plus loin en l'état.

En revanche, il faut distinguer les urgences concernant tout le marché intérieur, et celles qui frappent un État membre seulement. Dans ce dernier cas, la définition relève de la compétence nationale. On peut envisager l'obligation harmonisée de fixer une durée à l'urgence, mais aller au-delà risquerait de porter atteinte au principe de subsidiarité.

M. André Gattolin, rapporteur. - Peut-être pourrions-nous, à l'alinéa 68, mentionner parmi les exemples la notion d'une crise majeure. En outre, la proposition de règlement prévoit l'accès aux données pour prévenir -et non seulement traiter- une situation d'urgence. Le risque lié aux régimes d'exception me semble surtout important sur ce point.

Mme Catherine Morin-Desailly, rapporteure. - Selon le *c* du 1 de l'article 17 de la proposition de règlement, la durée d'utilisation des données doit être précisée. La répétition, même si elle est à la base de la pédagogie, est-elle bien nécessaire ?

M. André Reichardt. - Chat échaudé craint l'eau froide : nous voyons bien comment la deuxième vague pandémique, en France, avait conduit notre ministre de la santé à prolonger l'état d'urgence sanitaire, sous le prétexte effrayant d'une charge virale mille fois plus grande. L'autorité nationale peut prendre tout type de décision.

M. Jean-François Rapin, **président**. - Je ne vois pas l'autorité européenne s'y substituer.

M. André Reichardt. - Tout à fait, mais il s'agit de créer un garde-fou pour les autorités publiques, nationales comme européennes. Il faut selon moi préciser la notion d'urgence.

M. Jean-François Rapin, **président**. - À nouveau, j'alerte sur la nécessité de respecter le principe de subsidiarité.

M. André Gattolin, **rapporteur**. - Lors d'un déplacement sur place en septembre 2020, avec Jean Bizet et Jean-Yves Leconte, nous avions constaté que les décisions d'urgence prises en Hongrie ont annihilé la capacité des collectivités locales, notamment la mairie de Budapest, à exécuter leur budget, empêchant l'opposition à Viktor Orban de démontrer sa capacité à agir. Le recours à l'état d'urgence varie singulièrement d'un pays à l'autre.

Mme Catherine Morin-Desailly, **rapporteure**. - Nous n'avons pas vocation à définir l'urgence. Nous pourrions toutefois compléter l'alinéa 68 par les mots : « et que sa durée soit encadrée. »

M. André Gattolin, **rapporteur**. - Il faut en effet que la durée de telles mesures soit limitée.

M. André Reichardt. - Très bien.

Il en est ainsi décidé.

Mme Pascale Gruny. - Avec Laurence Harribey et Patricia Schillinger, nous travaillons actuellement sur la régulation en matière de données de santé. La protection des données de santé est fondamentale, mais celles-ci sont essentielles à la recherche. Tout en comprenant André Reichardt, je souligne l'importance de ne pas bloquer l'accès à ces données.

Mme Florence Blatrix Contat, **rapporteure**. - L'utilisation des données à des fins de recherche est déjà prévue dans le texte, et ce même en dehors de situation d'urgences.

M. Jean-François Rapin, **président**. - Nous sommes malheureusement très en retard sur les données de santé. Chaque application de santé prévoit des clauses d'acceptation par l'utilisateur du transfert de ses données, hors de tout contrôle…

Mme Catherine Morin-Desailly, **rapporteure**. - En principe, ces données sont anonymisées, mais les données françaises sont gérées par des acteurs extra européens. C'est pourquoi nous demandons que soit établie une liste des données sensibles. La Commission nationale de l'informatique et des libertés (Cnil) recommande d'ailleurs de trouver rapidement des solutions souveraines, qui sont à notre portée.

Mme Pascale Gruny. - La commission des affaires sociales travaille aussi sur ce sujet. La plateforme européenne attend la mise en oeuvre de la plateforme française.

L'anonymisation est associée au numéro d'inscription au répertoire (NIR, ou numéro de sécurité sociale), qui permet donc de retrouver la personne concernée. On risque de perdre l'anonymat. Les personnes auditionnées nous confirment qu'on ne pourra jamais se protéger de toutes les attaques conduites par des *hackers*.

M. Jean-François Rapin, **président**. - J'ajoute que le Sénat est attaqué depuis plusieurs jours. Soyez prudents… Vendredi, notre site était d'ailleurs inaccessible.

Mme Catherine Morin-Desailly, **rapporteure**. - André Reichardt demandait à préciser l'alinéa 29. Votre proposition de remplacer les mots : « n'est pas un service numérique lié à un objet connecté relevant » par les mots : « est exclu du champ » ne pose pas de souci. Appelons un chat un chat.

Il en est ainsi décidé.

M. Pierre Ouzoulias. - Je me réjouis que la commission des affaires européennes du Sénat soit pilote sur ces sujets complexes et irrigue les travaux des autres commissions. Après six ans, nous ne connaissons toujours pas la position du Gouvernement en la matière. Nous votons, deux à trois fois par an, des lois rendues obsolètes par les directives et règlements européens. Ainsi, le 12 juillet 2022, à l'occasion de l'examen du projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne, le Gouvernement m'avait assuré que les prochains règlements européens ne remettraient pas en cause le texte que nous votions. Tel n'a pas été le cas, et le projet de loi qui vient d'être déposé ne fait que prolonger cette incompréhension.

Je tiens beaucoup à votre mention de l'interopérabilité dans la proposition de résolution. Les citoyens doivent avoir une alternative lorsque leurs réseaux sociaux et *clouds* ne sont pas conformes à leurs valeurs. Or, aujourd'hui, nous en sommes prisonniers, car nous ne pouvons retirer nos données de ces opérateurs.

Enfin, nous ne pouvons faire l'économie d'une politique industrielle et d'investissements massifs.

M. André Gattolin, **rapporteur**. - Nous le disons depuis dix ans !

Mme Catherine Morin-Desailly, **rapporteure**. - Considérez-vous normal que les fournisseurs de service d'informatique en nuage continuent à formuler des offres gratuites, jusqu'à un certain seuil, pour appâter et enserrer le client ? Il est difficile de sortir de ce qui s'apparente à du *dumping*.

M. André Gattolin. - L'internet s'est fondé sur le mythe de la gratuité. Les entreprises se rétribuent sur les données, la publicité ou l'abonnement, voire, en position dominante, sur l'ensemble des vecteurs. La gratuité, en elle-même, pose problème dans un système concurrentiel dès lors qu'elle emprisonne le client. Lors de son audition, OVHcloud, nous a rappelé que cette technique d'enfermement l'empêche de prospérer dans les secteurs où il est le plus concurrentiel. La suppression progressive, sur trois ans, des frais de changement d'opérateur émane sans doute du *lobby* des grands groupes internet à Bruxelles.

J'ai demandé à la Commission européenne qui étaient réellement les membres de DIGITALEUROPE : à de rares exceptions près, comme Dassault Systèmes, ils étaient à 90 % américains. Désormais, les Chinois, avec TikTok et Huawei, y sont présents en force. Alors que, depuis la directive sur le commerce électronique, on refuse les barrières pour ne pas gêner le développement d'un internet européen, avec notamment le principe de non-

responsabilité des hébergeurs, on n'a fait que renforcer les opérateurs internationaux sur le marché européen.

Cependant, il ne fait pas de doute que la Commission est sous pression. Ainsi, lors des travaux sur la directive Vie privée et communications électroniques, les trente principaux cabinets d'avocats spécialisés dans le droit du numérique à Bruxelles étaient déjà sous contrat avec Google ou ce qui deviendrait Meta. Nous sommes juridiquement désarmés. La production du droit est en cours de « désouverainisation ».

Mme Catherine Morin-Desailly, rapporteure. - Seuls les Gafam - Google, Apple, Facebook, Amazon, Microsoft - peuvent proposer des offres véritablement gratuites. Ils captent les marchés par anticipation, notamment *via* l'Éducation nationale : c'est une concurrence déloyale au *cloud* européen. Je vous rappelle aussi que nos marchés sont ouverts aux quatre vents, quand ceux des États-Unis nous sont fermés. Sans symétrie, nous continuerons à scier la branche, déjà bien fragile, sur laquelle nous sommes assis.

M. Jean-François Rapin, président. - Le sujet émergent est celui des objets connectés. Un échelon est franchi avec la voiture autonome. On vous impose un opérateur, en général un Gafam, lors de l'achat du véhicule. Ainsi, un compte Google est requis pour faire fonctionner l'Austral de Renault. Nous sommes rattrapés par la patrouille, hors de toute réglementation.

Mme Catherine Morin-Desailly, rapporteure. - C'est tout l'enjeu des systèmes propriétaires.

M. André Gattolin. - Je souligne qu'il y a un défaut de vision globale en raison de l'emboîtement des législations européennes. Il est impératif de veiller à leur articulation..

La commission adopte la proposition de résolution européenne, ainsi modifiée, disponible en ligne sur le site du Sénat, ainsi que l'avis politique qui en reprend les termes et qui sera adressé à la Commission européenne et au Parlement européen, et autorise la publication du rapport d'information.

Proposition de résolution européenne sur la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données)
COM(2022) 68 final

Le Sénat,

Vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Programme de travail de la Commission pour 2020 - Une Union plus ambitieuse », COM(2020) 37 final,

Vu la 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 » du 19 février 2020, COM(2020) 66 final,

Vu la résolution du Parlement européen du 25 mars 2021 sur une stratégie européenne pour les données /2217(INI), (2021/C 494/04),

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques),

Vu la proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (directive vie privée et communications électroniques), COM/2017/010 final,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données - RGPD),

Vu la directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites,

Vu le 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,

Vu la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen,

Vu le 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),

Vu la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) COM(2022) 68 final,

Des objectifs pertinents

Considérant que la présence généralisée d'objets connectés dans les sphères privées et publiques produit de très nombreuses données dont la croissance est exponentielle ;

Considérant que ces données ouvrent des perspectives particulièrement prometteuses pour stimuler l'innovation dans de nombreux secteurs ;

Considérant que les utilisateurs des objets connectés et des services liés n'ont généralement pas accès, pour des raisons techniques et commerciales, aux données produites par l'utilisation de ces objets et services ;

Considérant que ces données sont souvent utilisées par leurs détenteurs à d'autres fins que celles qui en justifient le recueil et ce sans que les utilisateurs en soient pleinement informés ;

Considérant que les grands acteurs du numérique tendent à empêcher les micro, petites et moyennes entreprises d'accéder aux données dans des conditions satisfaisantes alors que ces données leur permettraient de développer de nouveaux services, dans un cadre concurrentiel équilibré ;

Soutient le principe de la mise en place d'une législation européenne horizontale définissant des règles harmonisées pour un accès équitable aux données produites par l'utilisation d'objets connectés et de services liés, et prévoyant des processus de règlement des litiges ;

Approuve en particulier l'objectif de transparence en matière de recueil de ces données et la reconnaissance de droits effectifs aux consommateurs et aux entreprises sur les données qu'ils produisent en utilisant des objets connectés et des services liés ;

Soutient également l'objectif d'un partage choisi de ces données avec des tiers, dans un cadre contractuel équilibré qui permet au tiers bénéficiaire de ne pas être soumis à des exigences excessives par le détenteur des données ;

Est également favorable à l'adoption de règles permettant de procéder effectivement à un changement de fournisseur de services de traitement des données et à l'encadrement des transferts internationaux de données à caractère non personnel ;

Estime toutefois que, pour atteindre ses objectifs, la proposition de règlement doit être précisée et complétée sur plusieurs points ;

Attire l'attention sur la nécessaire articulation de cette législation transversale avec les régimes sectoriels existants et à venir, par exemple en matière de données de santé ;

Souhaite, qu'au-delà de la reconnaissance des droits des consommateurs sur les données générées par les objets connectés et les services liés qu'ils utilisent, les règles européennes en matière de protection des consommateurs fassent l'objet d'une évaluation générale de leur pertinence

dans un environnement de plus en plus numérique et que des adaptions et compléments y soient apportés afin d'assurer une meilleure protection des consommateurs en ligne ;

Préciser le champ d'application du règlement

Considérant que la proposition de règlement concerne les données « générées par l'utilisation d'un produit, y compris incorporé dans un bien immeuble, ou d'un service lié » ;

Préconise qu'il soit indiqué explicitement qu'il s'agit de produits connectés, et, que les données concernées sont des données brutes, non modifiées ni ajoutées, résultant directement de l'utilisation de ces objets ou de services liés ;

Demande qu'il soit en outre précisé que le service de communication électronique, qui est régi par des textes spécifiques, est exclu de champ d'application de la proposition de règlement ;

Veiller à la primauté des règles de protection des données à caractère personnel

Considérant que les données recueillies par des objets connectés et des services liés peuvent inclure des données à caractère personnel ;

Considérant que le recueil et l'utilisation de telles données sont encadrés par plusieurs textes européens dont le RGPD et la directive vie privée et communications électroniques ;

Préconise qu'il soit précisé que la définition des données à caractère personnel susceptibles d'être présentes dans les données recueillies par des objets connectés et des services liés est celle du RGPD ;

Estime préférable qu'il soit expressément indiqué que, pour les données à caractère personnel figurant parmi les données recueillies, les règles européennes applicables en matière de données à caractère personnel prévalent en toute hypothèse sur les dispositions de la proposition de règlement, sous le contrôle de l'autorité nationale de protection des données compétente ;

Considérant que l'utilisateur de l'objet connecté peut ne pas être la personne dont des données à caractère personnel sont recueillies ;

Souligne qu'il convient d'être particulièrement vigilant en pareil cas et que le détenteur des données doit veiller à ce que la transmission de ces données à l'utilisateur soit effectuée dans le strict respect du RGPD ;

Renforcer la protection des droits des utilisateurs sur les données produites par l'utilisation d'objets connectés et de services liés

Considérant qu'il est proposé de reconnaître à l'utilisateur d'un objet connecté et de services liés un droit d'accès aisé, sécurisé et direct sur les données produites par l'utilisation qu'il fait de l'objet et des services liés ;

Considérant que cet accès devra être prévu techniquement dès la conception de l'objet connecté ;

Demande, pour que l'accessibilité soit effective, qu'il soit exigé que le format des données soit compréhensible, structuré, habituel et lisible par la machine, et que les métadonnées nécessaires à leur interprétation soient communiquées à l'utilisateur ;

Estime qu'il devrait également être précisé que, lorsqu'elles ne sont pas directement accessibles, les données doivent être mises à la disposition de l'utilisateur sans délai indu et présenter une qualité technique équivalente en termes de réutilisation, de sécurité et de format ;

Considérant que la proposition de règlement prévoit que l'utilisateur soit informé, préalablement à l'acquisition de l'objet connecté et des services liés, des données que leur utilisation produira, des modalités d'accès à ces données, de l'utilisation qui en sera faite et de leur éventuelle ouverture à un tiers ou encore du droit d'introduire une plainte auprès de l'autorité compétente ;

Considérant qu'elle prévoit également que l'utilisateur soit préalablement informé, le cas échéant, de l'existence de secrets d'affaires et de droits de propriété intellectuelle et de leurs conséquences pour l'exercice de son droit d'utiliser et de partager ces données avec un tiers ;

Considérant qu'il est prévu que le détenteur des données ne puisse utiliser celles-ci que dans le cadre d'un accord contractuel conclu avec l'utilisateur du produit connecté et des services liés ;

Considérant que la proposition de règlement prévoit qu'il est expressément interdit au détenteur des données d'utiliser celles-ci pour évaluer la situation économique, les actifs ou les méthodes de production de l'utilisateur ;

Préconise que soient identifiées des clauses qui porteraient une atteinte injustifiée aux droits de l'utilisateur en matière d'utilisation et de partage des données et que soit examinée l'opportunité de les interdire et de les priver d'effet ;

Faciliter le partage des données avec des tiers

Considérant que l'utilisateur d'un objet connecté ou de services liés est en droit de demander au détenteur des données ainsi générées que celles-ci soient mises à la disposition d'un tiers ;

Considérant que la proposition de règlement prévoit que les contrôleurs d'accès soient exclus du bénéfice, direct ou indirect, d'un tel partage de données ;

Estime que cette exclusion est justifiée au regard du pouvoir de marché excessif de ces opérateurs ;

Considérant que la proposition de règlement prévoit que les micro et petites entreprises ne soient pas soumises à l'obligation de mise à disposition des données sauf si elles ont des entreprises partenaires ou des entreprises liées ;

Estime que les micro et petites entreprises ayant un lien avec un fabricant de produits connectés ou un fournisseur de services liés devraient également être soumises à cette obligation ;

Invite à l'ouverture d'une réflexion sur la pertinence de l'application des seuils de droit commun en termes de chiffres d'affaires, de bilan et de nombre de salariés pour qualifier ces entreprises, et sur l'opportunité de prendre en compte à cet effet le nombre de données générées par les objets connectés et services liés qu'elles mettent à disposition ;

Considérant que la proposition de règlement prévoit que le détenteur des données qui met celles-ci à la disposition d'un tiers veille à leur qualité et à leur sécurité ;

Considérant que la proposition de règlement prévoit que les conditions de cette mise à disposition convenues entre le détenteur des données et un tiers bénéficiaire doivent être équitables, raisonnables, non discrétionnaires et transparentes ;

Approuve le fait que certaines clauses qui réduisent l'accès de PME aux données et la possibilité de les utiliser soient prohibées et considérées comme inopposables;

Considérant que la proposition de règlement prévoit d'autoriser que la mise à disposition des données fasse l'objet d'une compensation raisonnable et non discriminatoire à la charge du tiers bénéficiaire dont le détenteur des données doit fournir les bases de calcul ;

Demande que, pour prévenir les risques d'abus, la marge qui peut être facturée au tiers bénéficiaire soit plus précisément encadrée que par la seule exigence d'un caractère raisonnable et non discriminatoire ;

Veiller à une protection équilibrée des secrets d'affaires et prendre en compte les impératifs de sécurité

Considérant que la proposition de règlement prévoit que le détenteur des données et l'utilisateur du produit connecté et de services liés doivent s'accorder sur les mesures techniques et opérationnelles à mettre en place pour assurer la protection des secrets d'affaires avant l'ouverture des données ;

Considérant qu'elle indique que de de telles mesures doivent également être prévues en cas de partage des données avec un tiers ;

Considérant que la proposition de règlement interdit expressément à l'utilisateur et au tiers bénéficiaire d'utiliser les données recueillies pour développer des produits concurrents ;

Souligne que le cadre contractuel de protection de secrets d'affaires susceptibles d'être révélés par des données brutes en cas de demande d'accès et de transmission de celles-ci doit être équilibré et ne pas excéder les exigences de protection de tels secrets ;

Estime toutefois que la protection des secrets d'affaires doit pouvoir exceptionnellement justifier un refus de transmettre les données, y compris à l'utilisateur, si le détenteur des données démontre que leur divulgation est de nature à avoir des conséquences dommageables sérieuses, y compris au regard de la sécurité ;

Encadrer l'accès d'autorités publiques nationales et européennes à des données en cas d'urgence publique

Considérant qu'aux termes de la proposition de règlement, les détenteurs de données pourraient être dans l'obligation, en cas d'urgence publique, de mettre des données générées par l'utilisation d'objets connectés et de services liés à la disposition d'un organisme public national ou de l'Union européenne démontrant un besoin exceptionnel d'utiliser ces données pour faire face à une urgence, prévenir une telle urgence ou pour contribuer au rétablissement à la suite d'une telle urgence ;

Considérant que l'urgence publique est définie par la proposition de règlement comme « une situation exceptionnelle ayant une incidence négative sur la population de l'Union, d'un État membre ou d'une partie de celui-ci, entraînant un risque de répercussions graves et durables sur les conditions de vie ou la stabilité économique, ou la détérioration substantielle d'actifs économiques dans l'Union ou dans les États concernés » ;

Souhaite que soient précisées la nature de l'urgence, pour viser expressément diverses circonstances (santé, catastrophe naturelle, catastrophe majeure d'origine humaine, cyberattaque), ses conséquences (y compris sur la stabilité financière ou des actifs économiques majeurs) et que sa durée soit encadrée ;

Estime que l'obligation d'ouverture des données hors cas d'urgence publique, lorsque l'absence de données disponibles empêche l'organisme ou l'institution publics de s'acquitter d'une mission spécifique d'intérêt public, doit être précisément encadrée, en particulier sa durée et sa portée, afin de ne pas priver abusivement des entreprises des bénéfices qu'elles peuvent légitimement retirer de l'exploitation des bases de données qu'elles ont constituées ;

Souligne que cette mise à disposition ne doit être requise que si les autorités publiques concernées justifient qu'elles ne sont pas en mesure d'obtenir rapidement ces données par d'autres moyens ;

Demande qu'il soit précisé que les organismes publics ne peuvent utiliser les données que pour la seule finalité de la demande, et dans le strict respect des droits et libertés des personnes, en particulier lorsqu'il s'agit de données à caractère personnel qui ne peuvent être anonymisées ;

Renforcer l'effectivité du droit de changer de fournisseur de services de traitement des données

Considérant que les principaux fournisseurs de services de traitement actifs en Europe sont de très grandes entreprises étrangères qui exercent une position dominante sur le marché intérieur et ont développé des pratiques pour empêcher leurs utilisateurs d'utiliser d'autres logiciels que ceux qu'elles proposent et de se tourner vers d'autres fournisseurs ;

Considérant que la proposition de règlement entend supprimer les obstacles commerciaux, techniques et contractuels au changement efficace de fournisseur de services de traitement des données ;

Demande que le fournisseur de services de traitement des données soit tenu de communiquer, préalablement à l'acceptation de l'offre de traitement des données, des informations précises sur les conditions, coûts et modalités de changement de fournisseur;

Souhaite qu'il soit expressément indiqué que le transfert des données ne doit pas pouvoir être refusé ou retardé lorsque le client a bénéficié d'une

offre d'utilisation gratuite des services de traitement des données ;

Estime que la complexité technique de ce transfert et de la période transitoire ainsi que l'impératif de continuité du service exigent une information précise du client sur les étapes techniques du processus de changement de fournisseur et les droits et obligations des différentes parties ;

Considérant qu'il est prévu que la suppression progressive des frais de changement de fournisseur s'étale sur trois ans à compter de l'entrée en vigueur du règlement ;

Estime qu'en raison de sa durée un tel délai est de nature à empêcher les fournisseurs de services européens de développer leur présence sur le marché intérieur qui est de plus en plus dominé par de grands acteurs étranger ;

Veiller au respect des valeurs et des intérêts européens dans les flux internationaux de données

Considérant que les transferts internationaux de données ne doivent pas exposer les données à un risque d'être rendues accessibles à des autorités étrangères qui ne seraient pas liées aux États européens par un accord international assurant la protection des données à caractère personnel, de la propriété intellectuelle, des secrets d'affaires, des engagements de confidentialité et des données commercialement sensibles ;

Considérant que la proposition de règlement fait obligation aux fournisseurs de services de traitement de données de vérifier la licéité de toute demande d'accès ou de transfert de données non personnelles émanant d'une autorité étrangère, de s'assurer de sa proportionnalité et de l'existence d'une possibilité de contestation devant une juridiction compétente du pays tiers ;

Considérant qu'il est prévu que le fournisseur destinataire d'une telle demande doit consulter les autorités ou organismes compétents notamment lorsqu'il estime que la décision peut concerner des données commercialement sensibles ou porter atteinte aux intérêts de l'Union, ou de ses États membres en matière de sécurité nationale ou de défense ;

Considérant que la proposition de règlement impose aux fournisseurs de prendre toutes les mesures techniques, juridiques et organisationnelles raisonnables, y compris des accords contractuels, afin d'empêcher l'accès aux données et leur transfert à des autorités d'États tiers qui ne seraient pas liés par un tel accord dès lors que cet accès ou ce transfert serait contraire au droit de l'Union ou d'un État membre ;

Approuve la définition de règles dictées par le souci d'assurer le respect des valeurs et des intérêts européens dans les flux internationaux de données ;

Demande que soit établie une liste des données sensibles (dont les données de santé) et des données dont la divulgation est susceptible de porter atteinte à la sécurité nationale, pour lesquelles un hébergement souverain est nécessaire afin de les protéger d'une application extraterritoriale de législations extra-européennes ;

Souligne que le caractère souverain exige en particulier que le service soit fourni par une entreprise européenne dans laquelle les participations étrangères cumulées, directes ou indirectes, ne peuvent être que marginales ;

Développer des normes en matière de portabilité et d'interopérabilité des données

Considérant que l'interopérabilité des données et leur portabilité sont nécessaires pour pouvoir échanger et utiliser les données d'espaces et de systèmes de données distincts ;

Considérant qu'il est prévu que des actes d'exécution seront pris par la Commission pour définir des règles harmonisées en la matière ;

Invite à préciser plus avant l'objet de ces normes harmonisées d'interopérabilité et de portabilité des données et à en détailler le processus d'élaboration, en particulier le rôle des États membres et des organismes de normalisation ;

Veiller à l'efficacité de la supervision de la mise en oeuvre du règlement

Considérant que les États membres doivent désigner les autorités nationales compétentes pour suivre la mise en oeuvre du règlement, traiter les réclamations et infliger des sanctions en cas de manquement ;

Attire l'attention sur la nécessaire coordination au sein des États membres entre les différentes autorités nationales, en particulier les autorités compétentes en matière de protection des données à caractère personnel ;

Préconise que les autorités nationales compétentes soient dotées de la possibilité d'imposer des remèdes en cas de non-respect des obligations prévues par le règlement ;

Demande qu'une structure de coordination intra-européenne soit mise en place pour faciliter la mise en oeuvre du règlement.

Invite le Gouvernement à faire valoir cette position dans les négociations.

La réunion est close à 10 h 15.