

N° 140
SÉNAT

SESSION ORDINAIRE DE 2022-2023

16 juin 2023

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*

*Est devenue résolution du Sénat, conformément à l'article 73 quinquies,
alinéas 2 et 3, du Règlement du Sénat, la résolution adoptée par la
commission des affaires économiques dont la teneur suit :*

Voir le numéro :

Sénat : 596 (2022-2023).

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 » du 29 janvier 2020, 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 (2020/2217(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 (règlement « 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 adaptations 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 du 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 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 étrangers ;

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 œuvre du règlement :

Considérant que les États membres doivent désigner les autorités nationales compétentes pour suivre la mise en œuvre 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 œuvre du règlement ;

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

Devenue résolution du Sénat le 16 juin 2023.

Le Président,

Signé : Gérard LARCHER