ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Mission d'information de la Conférence des Présidents « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

– Audition, ouverte à la presse, de M. Jean-Luc Sauron, professeur associé à l'université de Paris-Dauphine..... 2

Mardi
25 mai 2021
Séance de 10 heures 5

Compte rendu n° 76

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Philippe Latombe, rapporteur

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Jean-Luc Sauron, professeur associé à l'université de Paris-Dauphine.

Présidence de M. Philippe Latombe, président et rapporteur

La séance est ouverte à dix heures cinq.

M. Philippe Latombe, président et rapporteur. M. Jean-Luc Sauron, vous êtes professeur associé en charge du diplôme de délégué à la protection des données de l'université de Paris-Dauphine.

Nos auditions ont souvent traité du modèle européen du numérique, parfois qualifié d'humaniste et en tout cas distinct tant du modèle américain marqué par la prévalence de l'absence d'entraves à l'activité économique que d'un modèle autoritaire donnant à la souveraineté numérique l'aspect d'un suivi très attentif, voire soupçonneux, de l'usage d'Internet par les citoyens. Il a été question de convertir ce modèle européen en un outil, d'abord de puissance et de régulation au service du *soft power*, puis, un temps, d'une volonté de rééquilibrage de la compétition industrielle et économique. Nous comptons sur votre éminente connaissance des arcanes de la construction européenne pour nous éclairer à cet égard.

Je vous poserai trois questions liminaires.

Ma première concerne votre approche de la notion de souveraineté numérique. Il s'agit là d'une question rituelle lors de nos auditions, procédant de la grande diversité des définitions données à cette notion. Comment vous-même la concevez-vous ? Ne tendons-nous pas à présumer que les autres États de l'Union européenne (UE) partagent une vision de la souveraineté numérique européenne alignée sur la nôtre ? Les États voisins de la France en nourrissent-ils une conception proche ou divergente ?

Mon deuxième point portera sur l'évolution du droit européen des données personnelles. Comment évaluez-vous la portée de la jurisprudence récente, dont l'arrêt de la Cour de justice de l'Union européenne dit « Schrems II », du point de vue, tant de la garantie des droits de la personne, que de la réponse la plus efficace possible aux prétentions de certaines institutions publiques américaines d'user de leurs prérogatives hors du territoire des États-Unis ? Que répondre aux inquiétudes qui s'expriment parfois d'un risque induit de désavantage relatif dans la compétition scientifique et industrielle en matière, par exemple, d'Intelligence artificielle ? Comment pourrions-nous, en Europe, réguler sans entraver l'innovation ?

Je m'attacherai en troisième lieu aux initiatives de la Commission européenne en vue d'encadrer juridiquement l'espace numérique européen. Le *Digital Services Act (DSA)* portant sur les services numériques tend surtout à renforcer le processus de contrôle des contenus, tandis que le *Digital Markets Act (DMA)* visant les entreprises du numérique veut instaurer une nouvelle régulation du comportement des grandes plateformes sur le marché européen. Enfin, le *Data Governance Act (DGA)* s'efforce de consolider le cadre juridique du marché européen de la donnée. Comment jugez-vous ces initiatives en l'état, sachant que les trilogues où l'on en débattra n'ont pas encore commencé ?

M. Jean-Luc Sauron, professeur associé à l'université de Paris-Dauphine. En préparant cette audition, j'ai été frappé par la multiplicité des définitions données à la

souveraineté numérique. Cette multiplicité montre bien l'extrême difficulté qui surgit pour qui tente de cerner cette notion, d'autant que certains refusent d'en considérer la polyvalence.

Sa meilleure définition reposerait encore, à mon sens, sur celle du cadre dans lequel elle s'exerce. M. Thierry Breton, en 2019, a évoqué le sujet lors d'une audition devant le Sénat. Il a très justement choisi de définir la souveraineté numérique comme un espace informationnel, de même qu'il existe un espace territorial, maritime ou encore aérien. Cette notion, extrêmement mouvante, d'espace informationnel recouvre l'ensemble considérable et sans cesse croissant des informations que les citoyens, les administrations et le secteur économique produisent et traitent.

La notion de souveraineté, appliquée à un État ou une nation, suppose en principe celle de frontières, qui me paraît difficile à transposer dans le domaine du numérique, encore qu'il ne faille pas écarter cette possibilité. La souveraineté repose aussi sur l'idée d'un pouvoir détenu par l'autorité publique dans un espace, en l'occurrence informationnel, pour organiser celui-ci, le structurer et le défendre. Il me semble en tout cas qu'il ne saurait exister de souveraineté numérique de l'espace informationnel sans stratégie nationale ou européenne pour le construire, sans anticipation de son devenir et sans outils pour le transformer. L'anticipation doit constituer un préalable à la stratégie, dont la mise en œuvre passera par des outils adaptés.

Je ne parviens pas, ce qui ne laisse d'ailleurs pas de me frapper, à discerner de stratégie numérique réelle en Europe, sauf depuis la récente nomination de M. Thierry Breton au poste de commissaire chargé, entre autres, du numérique. Nous nous contentons, jusqu'ici, en Europe, de naviguer à vue, en réaction à la conjoncture.

Nous avons d'abord réagi à notre environnement numérique par la convention 108 (pour la protection des données à caractère personnel) sous l'égide du Conseil de l'Europe, puis par la directive 95/46/CE (sur la protection des données). Le délai de transposition de cette directive courait jusqu'à octobre 1998. Or Google a été créée en septembre 1998. Nous constatons donc un décalage entre la réalité du monde numérique et notre législation européenne. Il a fallu attendre près de dix ans la mise en œuvre d'un outil, certes considérable, mieux adapté au contexte économique réel, tel que le Règlement général pour la protection des données (RGPD).

Il nous manque, selon moi, tant en France que dans l'Union européenne, la capacité d'anticiper. Avant de construire une stratégie et de concevoir les outils utiles à sa mise en œuvre, il faut réfléchir à ce que nous réserve l'avenir. Nous devons, à mon avis, nous appuyer sur ces trois piliers que constituent l'anticipation, la stratégie et les outils, pour viser un objectif de souveraineté numérique.

Vous m'avez interrogé sur l'existence d'une politique commune à l'Union européenne. Les 27 États qui la composent ne disposent pas tous d'une stratégie nationale de la donnée vraiment définie. La Grande-Bretagne, qui en avait une, a malheureusement quitté l'Union européenne. La France, l'Allemagne, l'Espagne et l'Italie en ont une également, mais l'on ne saurait en dire autant de tous les pays d'Europe. La seule limite que l'on constate, depuis près de vingt ans, aux politiques de la donnée vient de leur concrétisation industrielle.

En 2008, le programme Quaero ambitionnait de créer ce que l'on présentait alors comme un Google européen. Le partenaire allemand de ce projet franco-allemand s'en est

retiré en 2013 et l'aventure s'est soldée par un échec. L'actuel projet GAIA-X, franco-allemand à l'origine, a depuis intégré certains opérateurs issus de géants américains du numérique et même une société chinoise. Faute, là encore, de stratégie industrielle claire, cette initiative est devenue illisible. Faut-il s'appuyer sur les grands acteurs étrangers, quitte à nouer avec eux des partenariats ? L'Europe peut-elle encore rattraper son retard ? Ces questions méritent d'être tranchées. J'estime l'Union européenne capable de combler son retard, encore faut-il qu'elle s'en donne les moyens intellectuels.

Votre application du terme « humaniste » au modèle numérique européen m'a frappé tout à l'heure. Le RGPD veille avant tout à ce que la valeur que représentent les données reste là où elle est produite. Ne rejouons pas un combat humaniste. Ce RGPD répond au défi que devait relever l'Europe d'associer la capacité de nourrir notre économie de données avec un souci de la protection de ces mêmes données et du respect de la vie privée. Les États-Unis partagent ces mêmes préoccupations. Il me semblerait excessif de prétendre que les États-Unis foulent aux pieds les droits de l'homme. La remarque ne vaut certes pas pour d'autres systèmes, dictatoriaux.

Il me paraît tout de même étonnant de qualifier d'humaniste la protection des données en Europe. Une telle assertion revient à se tromper sur l'essence même du RGPD et de tout ce que nous avons construit depuis quarante ans.

M. Philippe Latombe, rapporteur. Cette assimilation erronée de la volonté de légiférer à un souci d'humanisme ne vient-elle pas du fait que la Cour de justice de l'Union européenne a rendu ses arrêts *Schrems* I, *Schrems* II et Tele2 dans un sens de protection des libertés individuelles et publiques ?

M. Jean-Luc Sauron. Il ne faut pas mettre sur le même plan les arrêts *Schrems* I et II, Tele2 ou même Quadrature du net, qui n'ont rien à voir. Ces arrêts s'inscrivent dans l'histoire des institutions européennes.

L'arrêt *Schrems* I a été rendu en 2015, c'est-à-dire avant l'entrée en vigueur du RGPD. L'activiste Max Schrems a en réalité attaqué le monopole de la Commission sur la définition d'une législation congruente. L'accord *Safe Harbor* de 2015, premier texte de relation entre les États-Unis et l'Union européenne, portait sur la protection des données lors de leurs échanges. En principe, une fois que la Commission européenne, à l'issue d'un long processus, prend une décision d'adéquation, selon laquelle un État tiers dispose d'une législation essentiellement convergente avec la nôtre en matière de données, il devient possible d'échanger celles-ci sans contrôle. Par son arrêt *Schrems* I, la Cour de justice européenne a remis ce principe en cause. Si jamais l'autorité de contrôle saisie par un citoyen prouve qu'en réalité, la législation de l'État tiers ne comporte pas les mêmes garanties de protection des données que notre législation, alors il revient à la Cour de justice de trancher la question. L'arrêt *Schrems* I a ainsi annulé l'accord *Safe Harbor*. Je vous rappelle que les législateurs, dont vous faites partie, ont intégré cette disposition à la révision de 2003 de la loi Informatique et libertés.

Le chapitre 5 du RGPD interdit clairement tout transfert de données vers un État extérieur à l'Union européenne, sauf, en vertu de son article 44, quand ces données bénéficient de la même protection hors du territoire de l'Union européenne. L'article 45 porte sur les décisions d'adéquation, l'article 46, sur les conventions internationales et autres outils garantissant la conformité de la protection des données, l'article 48 sur l'interdiction de

communiquer des données à des administrations de pays tiers et l'article 49, sur les cas dérogatoires. De fait, cet article 49 compte parmi ceux qui suscitent le plus de débats. Il se voulait une porte de sortie. En réalité, il ne concerne pas de flux importants de données mais uniquement des cas exceptionnels limités.

Pour qui l'arrêt *Schrems* II a-t-il des conséquences ? Pour n'importe quel utilisateur de FaceBook, de WhatsApp, ou encore de Zoom, comme vous et moi en ce moment, mais également pour l'ensemble des entreprises. À l'heure actuelle, il n'existe pas de solution qui permette de surmonter les difficultés soulevées par l'arrêt *Schrems* II. Les lignes directrices du comité européen de la protection des données (CEPD) ne répondent pas à la question fondamentale, qui porte sur la possibilité d'un recours juridictionnel pour assurer l'opposabilité des droits. La législation américaine n'est pas compatible avec la règlementation européenne. Comment des clauses contractuelles pourraient-elles aller à l'encontre de textes législatifs ? C'est impossible. Seul un nouvel accord entre les États-Unis et l'Union européenne serait en mesure de répondre à l'arrêt *Schrems* II.

L'arrêt Quadrature du net, relatif aux libertés publiques, met en lumière un problème de compatibilité avec un certain nombre de problématiques nationales. J'aimerais y revenir plus tard. Quoi qu'il en soit, il ne faut pas tout confondre.

L'arrêt *Schrems* II importe surtout par ses conséquences. Il n'existe pas aujourd'hui de société commerciale échangeant des données avec les États-Unis qui respecte le droit. La remarque s'applique à tous les secteurs, dont celui des banques. Y a-t-il lieu de le regretter ? Je ne le pense pas. Le juge de l'Union européenne a fait son travail. Il en a conclu qu'en l'état, le RGPD est inapplicable. Si les juridictions européennes ne parviennent pas à répondre aux difficultés que pose l'arrêt *Schrems* II, alors à quoi sert le RGPD ? En l'absence de réponse politique et juridique à l'arrêt *Schrems* II, je n'aurai plus qu'à mettre un terme à la formation diplômante que j'encadre pour me remettre au droit canonique.

M. Philippe Latombe, rapporteur. Justement, quelle solution opérationnelle pourrait être apportée à l'arrêt *Schrems* II ? Les équivalents, dans les autres pays européens, de la commission nationale de l'informatique et des libertés (CNIL) ont pris position sur le sujet, notamment son homologue irlandaise, qui en a tiré des conséquences assez strictes.

M. Jean-Luc Sauron. Je ne vois qu'une seule solution : un accord entre les États-Unis et l'Union européenne. Des négociations suivent d'ailleurs leur cours. Un tel accord devrait reconnaître la possibilité pour les ressortissants européens d'accéder aux juridictions américaines afin de faire valoir l'opposabilité de leur droit. Un tel accord interfèrerait avec les principes américains mais aussi avec le *Foreign Intelligence Surveillance Act (FISA)* et le *Patriot Act*.

Cela m'agace particulièrement que, parmi les décisions, articles et commentaires qui me tombent entre les mains, je n'aie pas encore trouvé une seule analyse vraiment pertinente et complète de la législation américaine, qui bloque l'exercice de nos droits et a suscité l'arrêt *Schrems* II.

Le mémoire de la CNIL relatif à l'ordonnance Health Data Hub indique clairement que l'entreprise qui reçoit une demande de communication de données émanant d'une agence de sécurité américaine ne peut pas en faire état à un tiers. Or cela ne dérange apparemment personne.

Vous avez auditionné les représentants d'Amazon Web Services (AWS). Que vous ont-ils dit ? Ils ont affirmé qu'au cas où une administration américaine leur adresserait une demande de communication de données, ils minimiseraient les données transmises. Il subsiste sur ce sujet beaucoup d'à-peu-près et de zones d'ombre, dont il faut sortir pour que se mobilise l'ensemble des juristes et de la communauté légale, composée des parlementaires et du gouvernement. Pourriez-vous me citer un seul gouvernement européen qui ait pris position sur l'arrêt *Schrems* II et ses conséquences ? L'attitude générale pourrait se résumer ainsi : « Cachez cet arrêt que je ne saurais voir. »

M. Philippe Latombe, rapporteur. Comment percevez-vous, à la lumière de l'arrêt *Schrems* II, les positionnements récents du gouvernement sur le Health Data Hub (HDH) et la doctrine du *cloud*, publiée voici quelques jours ?

M. Jean-Luc Sauron. Je serai franc : si seulement il n'y avait que le HDH à être hébergé par un *cloud* américain ! Demandez plutôt au gouvernement quels sont, en dehors de quelques opérateurs régaliens, les partenaires *cloud* de l'administration française.

Au lendemain de l'ordonnance de référé du Conseil d'État, très précisément la semaine suivante, l'Union des groupements d'achats publics (UGAP) claironnait un partenariat avec Microsoft Azure. Les quantités de données économiques, financières et d'organisations qui transitent par l'UGAP, centrale d'achat de l'administration, ne présentent-elles pas, à votre avis, un intérêt pour des tiers ?

Je n'ai pas compris, à la lecture des documents publiés par le gouvernement, en quoi notre *cloud* souverain assurerait notre souveraineté. Une demande de partenariat a été lancée dans l'idée de bénéficier des avancées technologiques des géants du numérique américains. Le problème du *cloud* souverain vient d'un défaut d'anticipation. Lors de son audition devant le Sénat en 2019, M. Thierry Breton, à l'époque, président-directeur général d'Atos, a déclaré que, pour l'heure, 80 % des données se trouvent dans le *cloud*. Le développement de l'Internet des objets, grâce auquel les objets connectés passeront, d'ici dix ans, de 23 milliards à 75 milliards, soit une moyenne de 10 par habitant, et plus encore dans les pays développés, entraînera une modification de la répartition des données. Le *cloud* n'en hébergera plus, alors, que 20 %. Qu'est-ce qui prendra de l'importance ? L'*edge computing* (informatique en périphérie), basé sur l'utilisation de la puissance de calcul là où se trouvent les données, c'est-à-dire, non plus dans le *cloud*, mais dans les objets connectés eux-mêmes. L'enjeu portera donc sur les algorithmes et, marginalement, la 5G (cinquième génération des standards pour la téléphonie mobile). Or les annonces de l'État concernent aujourd'hui le *cloud* souverain.

Je ne sais ce qu'il en est pour vous, mais j'ai, quant à moi, le sentiment très français que nous accusons systématiquement un retard. Il ne sert à rien de construire un *cloud* souverain, sorte de ligne Maginot numérique, alors que la bataille se jouera sur la maîtrise des algorithmes.

Comment les Américains et les Chinois ont-il construit leur avancée technologique ? À partir du bassin de données à leur disposition. Ces deux puissances vont développer grâce à ce bassin des algorithmes utilisés par l'Intelligence artificielle. Je suis bien sûr attaché aux droits fondamentaux et aux libertés individuelles et je défends le RGPD mais, faute d'un espace européen de la donnée, nous n'aboutirons à rien. Les différents pays de l'Union

européenne n'utilisent même pas les mêmes applications de contrôle du Covid. Si nous voulons rattraper notre retard et devenir autonomes, technologiquement, nous devrons, une fois établi le bassin de données qui nous manque, produire des systèmes d'Intelligence artificielle.

Ce que nous avons connu à propos de la 5G, au développement de laquelle n'a participé qu'un malheureux opérateur européen, se reproduira à une échelle dix fois supérieure dans le domaine de l'Intelligence artificielle et des algorithmes. Nous en revenons au défaut d'anticipation. Que ferons-nous dans cinq ans ? Où en serons-nous dans dix ans ? Nous devons accélérer et nous fixer des objectifs.

La réponse opérationnelle à la circulation des données comporte deux volets. Tout d'abord, il faut résoudre le problème soulevé par l'arrêt *Schrems* II. En 2019, le Conseil de l'Union a été mandaté pour discuter avec les États-Unis des relations entre nos autorités publiques respectives. Par le *Clarifying Lawful Overseas Use of Data Act* (*Cloud Act*), le gouvernement américain s'est arrogé le droit de consulter les fichiers d'entreprises soumises à la législation américaine, y compris à l'étranger.

Le deuxième volet du *Clourd Act*, tout aussi important, bien qu'il en soit peu question, prévoit des négociations internationales avec des États tiers pour assurer, dans un cadre légal, des relations entre autorités publiques. En somme, le *Cloud Act* n'est qu'une façon de contourner les traités d'entraide judiciaire. Une fois que certains pays se seront mis d'accord avec les États-Unis, ceux-ci iront piocher dans les données traitées par les opérateurs pour obtenir celles que nécessitent certaines enquêtes policières ou judiciaires.

Comment est né le *Cloud Act* ? Il ne vient pas d'un projet américain de domination du monde. Il a vu le jour parce que, dans le cadre d'une enquête policière, il a été demandé à Microsoft de fouiller dans des fichiers en Irlande. L'entreprise a objecté au gouvernement américain qu'elle n'y était pas autorisée à moins de méconnaître la souveraineté irlandaise. Quelques mois plus tard, le vote du *Cloud Act* a donné à Microsoft le droit de fournir au gouvernement les données nécessaires à une enquête relative à la sécurité nationale.

La réponse à l'arrêt *Schrems* II réside en un accord entre l'Union européenne et les États-Unis, qui apporte des garanties essentielles, communes aux deux espaces, en matière d'échange de données. Comment faciliter sa mise en œuvre ? Une loi française de 1968 interdit la communication à des États de données économiques, financières ou administratives. Les sanctions en cas de contravention sont aujourd'hui inexistantes, alors que les géants américains du numérique ne sont pas toujours en adéquation avec le gouvernement américain. Ils pourraient très bien objecter à un juge américain qu'au cas où ils communiqueraient aux États-Unis des données au mépris de lois étrangères, ils subiraient telle ou telle sanction. Ce juge, estimant ces sanctions trop pénalisantes, admettrait alors le refus de l'entreprise de transmettre les données demandées. En 1987, la Cour suprême américaine a clairement déclaré qu'en l'absence de sanctions effectives en cas de contravention à la loi de blocage française de 1968, celle-ci n'avait pas à être prise en compte. Pour faciliter les négociations avec les États-Unis, nous pourrions durcir les sanctions à l'encontre des grands opérateurs numériques. Rappelons que, depuis 2018, une seule condamnation a été prononcée en Europe contre un opérateur, par la CNIL. L'autorité italienne de régulation de la concurrence vient de lancer une procédure contre Google. Nous disposons d'outils, mais le plus efficace reste la négociation d'un accord international avec les États-Unis afin de définir les garanties essentielles qui nous permettraient d'avancer sur le sujet.

Il faut garder à l'esprit que la possibilité pour n'importe quel ressortissant européen ou étranger de défendre ses droits devant le juge est propre à notre culture européenne. Il n'en va pas de même aux États-Unis, en matière de traitement des données, ou alors très difficilement. Jusqu'à la décision d'adéquation entre l'Union européenne et le Japon, ce n'était pas possible non plus au Japon. Désormais, un ressortissant européen sollicitant une protection contre l'utilisation de ses données au Japon peut enfin, par le biais d'un mécanisme, certes assez lourd, mais qui a le mérite d'exister, obtenir une décision d'une juridiction japonaise. L'accès au juge, typiquement européen, n'est pas reconnu sur l'ensemble de la planète.

M. Philippe Latombe, rapporteur. Sur le plan opérationnel, ou plus exactement technique, que penser de GAIA-X, présenté comme l'une des réponses possibles à l'arrêt *Schrems* II ?

M. Jean-Luc Sauron. Pour le moment, GAIA-X a donné naissance à un partenariat entre OVHcloud et Deutsche Post. D'autres partenariats devront suivre. Rappelons que GAIA-X n'est pas un projet de *cloud* européen mais de moteur de recherche, censé fournir les références d'entreprises européennes répondant à un cahier des charges relatif à certains droits, aujourd'hui impossibles à appliquer, dans la pratique, par un opérateur européen de *cloud*. Ces droits concernent entre autres la portabilité ou la possibilité de transférer des données.

Aujourd'hui, le seul secteur où la portabilité des données s'est imposée reste celui des opérateurs téléphoniques, alors même que ceux-ci prétendaient une telle exigence impossible à mettre en œuvre. Un usager d'Orange peut ainsi migrer vers Bouygues tout en conservant son numéro de téléphone et ses données.

À ce jour, GAIA-X se résume à un cahier des charges, voire à une liste d'opérateurs. Le plus étonnant reste que, malgré l'arrivée récente de certains géants américains du numérique et d'opérateurs chinois dans l'initiative GAIA-X, ceux-ci ne bénéficieront pas du label GAIA-X, ce que je peine à comprendre.

J'ai bien saisi, en revanche, que deux campagnes se déroulent en ce moment au sujet du *DMA*. La rapporteure du Parlement européen, Mme Stéphanie Yon-Courtin, estime qu'il ne faut pas infléchir le *DMA* pour cibler les géants américains du numérique, alors qu'en réalité, si. Comment permettre à des plateformes européennes de monter en puissance, sinon en les protégeant de la concurrence des puissants acteurs américains ? Il ne sert à rien d'imposer un Règlement européen tant que les portes de l'Europe restent ouvertes à la concurrence étrangère.

J'y vois là une tare européenne. Il n'y a qu'en Europe qu'une société est considérée comme européenne, bénéficiant ainsi d'aides européennes, pour la simple raison qu'elle a établi une filiale sur le territoire de l'Union européenne. Les acteurs américains du numérique participent aux marchés publics européens. Pour qu'une entreprise européenne participe à un marché public au Canada, alors même que les opérateurs canadiens tels que Bombardier répondent déjà aux appels publics d'offres en Europe, il faudra attendre l'entrée en vigueur d'un accord commercial bilatéral de libre-échange (le *Comprehensive Economic and Trade Agreement* ou *CETA*).

La position défendue par cette rapporteure m'agace au plus haut point. Nous ne pouvons pas continuer comme cela. À quoi songe-t-elle ? Un problème de lutte se pose. L'un des points majeurs du *DMA* porte sur la possibilité de laisser à des plateformes européennes le temps de monter en puissance. Ensuite seulement, les règles de concurrence pourront changer, sans quoi aucune plateforme européenne n'émergera jamais. La fable de La Fontaine sur le lièvre et la tortue ne s'applique pas dans le monde économique.

Les autorités de concurrence nationales devraient en outre jouer leur rôle. Se sont-elles montrées capables d'une confrontation avec les géants américains du numérique ? Non. Il faut une force aussi importante que la Commission européenne pour intervenir sur le champ de bataille, où doivent être mobilisés bien plus que de petits régiments.

Le texte du *DGA* est d'une extrême importance, bien qu'il en soit peu question. Là encore, on note un manque de réflexion nationale et européenne sur ce que recouvre la notion de données ouvertes. Aujourd'hui, si vous me pardonnez la familiarité de cette expression, l'*open data*, c'est l'*open bar*. Les données ouvertes sont produites par les administrations, qui ne disposent ni de la réglementation ni des spécialistes seuls à même d'éviter que des tiers étrangers s'approprient leurs données économiquement utiles. Il aurait fallu, une fois de plus, anticiper l'usage de ces données ouvertes, source de richesse et de production de valeur. Qui en tire profit aujourd'hui ? Le secteur souffre d'une mauvaise structuration.

M. Philippe Latombe, rapporteur. Que devrions-nous, en tant que législateurs français, voire européens, mettre en œuvre pour améliorer la situation ? Que préconisez-vous, dans l'immédiat ?

M. Jean-Luc Sauron. Je n'ai jamais songé à dicter des lois, même dans mes rêves les plus fous. Différents secteurs sont à considérer.

D'abord, je réfléchirais à l'ensemble des autorités qui interviennent en France dans le domaine du numérique. Nous constatons dans notre pays une accumulation d'autorités administratives indépendantes. Dès qu'il s'en crée une, une autre s'y ajoute, aux compétences proches. Il faudrait remettre à plat ce champ et se donner les moyens d'agir. La CNIL accomplit un travail remarquable, mais elle n'emploie que 225 personnes. Vous n'imaginez bien évidemment pas qu'elle puisse, avec ce faible effectif, mener un travail de fond sur l'ensemble du territoire. Malgré la forte mobilisation de ses équipes, elle n'en a tout bonnement pas les moyens.

L'émission *Cash investigation* sur la carte vitale et l'utilisation des données de santé a suscité grand bruit, à juste titre. J'ai consulté la délibération afférente de la CNIL. On y lit en page 4 : *« Il est prévu que les personnes soient informées individuellement* [du traitement des données les concernant] *par la remise d'une notice d'information. »* Des délibérations dont nul ne vérifie l'application ne servent à rien. Il faudrait que la CNIL s'appuie sur un maillage du territoire comparable à celui de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

M. Philippe Latombe, rapporteur. Faudrait-il aller jusqu'à grossir le budget de la CNIL d'une partie des amendes qu'elle inflige ? Ou une telle proposition reviendrait-elle à tordre son modèle économique au risque de générer des effets de bord trop importants ?

M. Jean-Luc Sauron. Le système de la CNIL commence à dater. L'État pourrait se donner les moyens financiers d'assurer une régulation, dont l'importance économique n'est pas négligeable. Reconnaissons que ce serait contraire au mode de fonctionnement français et même européen. Le maillage du territoire revêt une importance considérable. L'acculturation au RGPD, et donc son application, ne progresseront qu'à condition d'y sensibiliser et d'y former les citoyens.

Le ministre actuel de l'éducation nationale effectue un travail considérable. Je ne le chargerai donc pas. J'estime toutefois aberrant de ne pas considérer l'éducation numérique comme un enjeu fondamental, au même titre que la capacité de lire, écrire et compter. La maîtrise des enjeux du numérique participe de la modification des modes de sélection dans l'administration et même l'emploi privé. Lors de mes études en droit, mes condisciples et moi-même devions acquérir des bases communes avant de nous spécialiser. J'estime impératif que des cours en université prolongent l'enseignement du numérique dans le primaire et le secondaire. Ces cours porteraient sur le RGPD et les grands principes du numérique, qui font désormais partie de la culture de tout honnête homme au XXI^{e} siècle.

Nous n'avons pas évoqué la Cour européenne des droits de l'Homme, dont la jurisprudence encadre pourtant aujourd'hui des pans entiers du domaine économique, concernant la protection des données.

Le fait, que des décisions prises dans un État de l'Union européenne ne s'appliquent pas dans les autres, me chagrine et choque quelque peu les opérateurs. En voici un exemple. L'autorité berlinoise de contrôle de la protection des données, suivie de ses homologues dans chacun des *Länder* allemands, a estimé, voici près de six mois la suite Microsoft 365 non conforme au RGPD. Il est inconcevable que des décisions portant sur des systèmes qui opèrent dans l'ensemble d'un espace de données, où celles-ci circulent sans frontières, jugent ceux-ci dangereux sur un territoire, alors que dans le territoire voisin, nul ne s'en émeut.

M. Philippe Latombe, rapporteur. Le problème de la cohérence entre les États européens vous semble-t-il le plus prégnant aujourd'hui ?

M. Jean-Luc Sauron. Sans conteste. La position des autorités de concurrence nationales, qui souhaitent aujourd'hui jouer un rôle dans l'application du *DMA*, relève selon moi d'un contresens historique.

M. Philippe Latombe, rapporteur. Je vous poserai maintenant la question rituelle qui conclut nos auditions. Souhaiteriez-vous aborder un sujet que nous aurions omis d'évoquer, ou insister sur un point particulier ?

M. Jean-Luc Sauron. D'abord, il me semble important de relever que certains droits n'existent pas dans la pratique. Je songe ici au droit à la portabilité, garanti par le RGPD, ou encore au droit au transfert de données, heureusement bloqué par l'arrêt *Schrems* II. Le droit à la portabilité garantit la liberté de choix du consommateur. Pour l'instant, il ne trouve d'application que chez les opérateurs de téléphonie mobile.

Ensuite, j'insisterai sur le problème de cohérence entre autorités administratives indépendantes. Hier, l'*Information Commissioner's Office (ICO)*, l'autorité britannique de contrôle du traitement des données, et la *Competition and Markets Authority (CMA)*, autorité

britannique de régulation de la concurrence, ont publié une déclaration de manière que leurs analyses convergent. Il ne me semble plus admissible que subsistent des incohérences dans la gestion d'un espace des données unique.

M. Philippe Latombe, rapporteur. La portabilité des données implique l'interopérabilité des systèmes et des plateformes.

M. Jean-Luc Sauron. En effet. Je souhaite bonne chance aux utilisateurs de Microsoft Azure pour exploiter leurs données dans un autre *cloud*.

M. Philippe Latombe, rapporteur. L'interopérabilité des systèmes s'avère donc indispensable, si l'on veut déposer des données chez un autre hébergeur.

M. Jean-Luc Sauron. Bien sûr, sinon l'utilisateur se retrouve prisonnier de son opérateur.

M. Philippe Latombe, rapporteur. J'aborderai le sujet avec les représentants de Microsoft jeudi.

M. Jean-Luc Sauron. Vous leur rappellerez les cris d'orfraie des opérateurs téléphoniques lorsque l'interopérabilité leur a été imposée. Tous ont juré qu'une telle exigence relevait d'une impossibilité technique, or ils sont finalement parvenus à s'y plier, en y mettant un peu de bonne volonté.

M. Philippe Latombe, rapporteur. Commercialement, ils l'ont ensuite présentée comme un avantage.

M. Jean-Luc Sauron. J'ai parfois l'impression que le secteur économique lui-même est en décalage avec la réalité. L'anticipation s'avère aussi nécessaire qu'une stratégie valable et les outils pour la mettre en œuvre. Nous l'avons déjà dit.

L'audition se termine à onze heures cinq.

Membres présents ou excusés

Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Réunion du mardi 25 mai à dix heures cinq

Présents. – Mme Marietta Karamanli, M. Philippe Latombe