ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France

Jeudi
26 mars 2026
Séance de 11 heures

Compte rendu n° 13

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures trente-cinq.

M. le président Philippe Latombe. Monsieur Schrems, je vous souhaite la bienvenue. Plusieurs arrêts des juridictions européennes portent votre nom. Pouvez-vous retracer l'histoire de vos différents combats pour la protection des données personnelles, qui vous ont notamment opposés à Facebook et à Meta ?

M. Max Schrems, fondateur de l'association NOYB (None of your business). Je vous remercie pour cette invitation.

Oui, cela fait longtemps que nous luttons. Tout a commencé quand Edward Snowden a dévoilé que le gouvernement américain avait accès à toutes les données hébergées sur le cloud américain, par les *hyperscalers*, tels qu'on appelle désormais les centres de données à très grande échelle.

Les États-Unis pratiquent une telle surveillance de masse depuis 2007 ; la section 702 de la loi Fisa (Foreign Intelligence Surveillance Act) qui a été introduite en 2008, a permis de légaliser cette pratique *a posteriori*. Les États-Unis ont ainsi un accès total à toutes les données qui sont soit la propriété d'un fournisseur de cloud américain, soit sous sa garde ou sous son contrôle, sans limite géographique. Cet accès concerne donc n'importe quel serveur sur la planète, dès lors qu'une société américaine y a accès de quelque façon que ce soit.

La section 702 de la loi Fisa distingue deux catégories de flux de données. La première concerne les citoyens et les résidents permanents américains – ceux que les Américains appellent les *US persons*. Ces flux bénéficient, au titre du quatrième amendement de la Constitution américaine, d'une protection qui est à certains égards plus forte que celle prévue en Europe et leur surveillance est jugée inconstitutionnelle.

Pour le reste – toutes les données qui ne concernent pas des citoyens ou des résidents permanents américains –, le gouvernement américain peut faire ce qu'il veut. Le problème concerne la grande majorité des Européens. Les États-Unis prévoient seulement un contrôle judiciaire annuel, pour s'assurer que, de manière générale, les flux de données concernant les *US persons* et les autres sont bien traités séparément. Le juge américain ne contrôle donc pas les collectes d'information sur un individu donné. Il a statué à deux reprises qu'il ne lui était pas possible de le faire.

Toutefois, à la suite d'intenses pressions politiques et économiques, l'idée s'est imposée qu'un nouvel arrangement était nécessaire concernant les transferts de données entre les États-Unis et l'Europe. C'est le Data Privacy Framework (cadre de protection des données). Celui-ci repose largement sur des garanties extralégislatives américaines – des courriers, des décrets présidentiels, et ainsi de suite –, car, en pratique, comme me le signalait un parlementaire américain, il serait impossible de faire adopter au Congrès américain une loi visant à accroître les droits des étrangers, pour des raisons politiques. Il n'est donc pas réaliste d'attendre des modifications de la législation américaine en ce sens.

Sur le plan des relations publiques, la Commission européenne a géré ces questions de manière très habile, se contentant de mentionner dans ses communiqués de presse la signature de nouveaux décrets, sans préciser que ceux-ci n'étaient souvent rien de plus qu'une copie directe de ceux signés sous la présidence de Barack Obama, dont les cours de justice avaient

signalé l'insuffisance. Il a souvent fallu un long travail d'analyse pour mesurer combien l'apport de nouveaux décrets était faible. Par exemple, la Commission européenne s'est félicitée que les États-Unis introduisent un principe de proportionnalité sur le modèle de celui prévu dans le droit européen, avec l'idée que cela permettrait d'interdire la surveillance de masse, dès lors que celle-ci est jugée disproportionnée par les tribunaux. Or ce n'est pas le cas. Interrogés sur ce point, les États-Unis expliquent ne pas avoir la même définition de la proportionnalité que l'Union européenne. Ainsi, les deux parties se sont accordées sur l'usage d'un terme, mais pas sur son sens. Votre recours, monsieur Latombe, permettra de clarifier ces questions.

Par ailleurs, la législation américaine est en train d'évoluer. La Cour suprême américaine, désormais très conservatrice, doit se prononcer dans les prochains mois sur les garanties d'indépendance dont dispose la Federal Trade Commission. Sa décision va probablement marquer la fin de toutes les autorités indépendantes aux États-Unis – alors que l'Union européenne s'est beaucoup appuyée sur leurs décisions pour assurer la protection des données de millions d'Européens. Les fondements des garanties actuelles pourraient être réduits à néant du jour au lendemain.

À la question de la surveillance s'est progressivement ajoutée, au cours de la dernière année, celle d'une possible fermeture de nos accès aux infrastructures par les États-Unis, dans différents domaines et pays. Après l'élection de Donald Trump, j'ai été invité au Danemark, en lien avec la menace pesant sur le Groenland : l'armée danoise s'inquiète qu'en cas de conflit avec les États-Unis, ceux-ci ne les privent de l'accès aux services numériques de Microsoft, AWS (Amazon Web Services) ou Google, par exemple. De fait, les États-Unis sont en mesure d'appliquer de tels embargos – ils le font actuellement à Cuba, en Syrie ou en Iran. Je suis un mondialiste et j'espère que ce type de situations ne se produira pas. Toutefois, au vu de ce qui s'est passé au cours de la dernière année, la question se pose. Les Danois s'inquiètent des conséquences qu'aurait un tel embargo – les hôpitaux, qui utilisent Microsoft, ne pourraient plus avoir accès aux dossiers, par exemple.

Au sein de l'Union européenne, la France a été précurseure pour lancer le débat sur la souveraineté. En tout cas, c'est au niveau européen qu'il faut fournir une réponse, parce que c'est seulement à cette échelle qu'il existe un marché suffisamment large pour justifier des investissements importants des entreprises. Il ne s'agit pas de garantir la souveraineté pour la souveraineté. Je suis un mondialiste et j'espère que dans le futur, tout le monde pourra travailler ensemble. Toutefois, il convient d'être réaliste : quand le monde est mû par le nationalisme, nous ne devons pas l'ignorer.

M. le président Philippe Latombe. Vous avez mené un travail important sur le train de mesures omnibus numérique proposé par la Commission européenne. Pourriez-vous le résumer ?

M. Max Schrems. Je tiens à votre disposition les analyses détaillées produites sur chaque article du paquet omnibus numérique par les avocats de notre association – le document fait 70 pages.

En résumé, selon nous, ce train de mesures poursuit deux buts différents. Une partie correspond à des mesures de simplification et de réduction de formalités administratives inutiles, que nous soutenons. Toutefois, des ajouts de dernière minute à ce paquet omnibus répondent à des impulsions politiques de la Commission et sont extrêmement problématiques, du point de vue de la protection de la vie privée – ils visent notamment à redéfinir la notion de données personnelles au point de la rendre obscure.

Notons que ces propositions posent également problème aux entreprises, car elles sont souvent floues et risquent de créer des difficultés pratiques. Par exemple, avec la dilution proposée de la notion de données personnelles, les données traitées par une compagnie A n'en relèveraient plus, quand celles traitées par une compagnie B en relèveraient encore, ce qui compliquerait la conclusion de contrats. Pour être franc, quel que soit le point de vue politique qu'on adopte, ces dispositions sont très mal rédigées et causeraient plus de problèmes et d'abus qu'elles n'apporteraient de solutions.

La majorité des États membres sont très sceptiques quant à la valeur des articles concernés. Ils risquent de les rejeter en bloc, ce qui nous semble une réponse raisonnable. Les spécialistes de ce domaine dans les ministères de la justice de chaque État membre sont parvenus à la même conclusion que nous : le travail sur certains de ces articles n'est pas abouti.

Mme Cyrielle Chatelain, rapporteure. Vous évoquez une impulsion politique de la Commission européenne derrière certaines dispositions du paquet omnibus numérique. Pour vous, est-ce dû au lobbying des entreprises de la Big Tech, qui est important à Bruxelles ?

Par ailleurs, pourriez-vous préciser quels sont les risques liés à la redéfinition de la notion de données personnelles pour les citoyens européens ?

Enfin, concernant les systèmes d'intelligence artificielle « à haut risque », le paquet omnibus numérique prévoit d'accorder aux entreprises un délai supplémentaire de mise en conformité. Actuellement, aux termes de l'AI Act (le règlement européen sur l'intelligence artificielle), le choix de classifier ou non un système d'IA comme étant « à haut risque » dépend d'une évaluation du fournisseur lui-même, mais celui-ci est soumis à des obligations de transparence. Le paquet omnibus numérique supprimerait ces normes de transparence, alors même que l'exploitation des données par des systèmes d'IA va gagner en intensité. Selon vous, ces changements sont-ils dus aux lobbys ? Pourriez-vous préciser les risques posés par l'IA pour les données personnelles et leur impact sur les citoyens européens ?

M. Max Schrems. Quand un député européen a demandé si, avec les modifications du RGPD (règlement général sur la protection des données) proposées par la Commission européenne, le traçage en ligne des individus, notamment à des fins publicitaires, serait toujours soumis aux obligations actuelles, celle-ci n'a pas pu apporter de réponse catégorique ; elle s'est contentée de répondre que cela dépendrait des cas. Cela montre bien comme les changements proposés sont risqués ! On pourrait donner une centaine d'exemples allant dans le même sens.

Les acteurs économiques du secteur souhaitent échapper – au moins partiellement – aux obligations du RGPD et certains des objectifs fréquemment avancés par leur groupe d'intérêts pour justifier ces demandes semblent raisonnables – la collecte de données à des fins de recherche, par exemple. Une solution qui permettrait de contenter tout le monde serait, non pas de renoncer au RGPD, mais de développer des techniques fiables d'anonymisation des données. Mais il faudrait pour cela définir l'anonymisation dans le RGPD – ce n'est pas le cas actuellement.

Je ne saurai pas répondre à votre question concernant l'AI Act, car notre organisation travaille surtout sur le RGPD. Nous ne traitons de l'intelligence artificielle que dans la mesure où elle pose des questions de protection des données personnelles. À ce titre, signalons toutefois que le paquet omnibus numérique prévoit d'introduire dans le RGPD un article 88 *quater* relatif à l'utilisation des données personnelles par l'IA. Cet article prévoit que, lorsque le traitement de données à caractère personnel est nécessaire dans le cadre du développement et de l'exploitation d'un système d'IA, il pourra être réalisé « aux fins d'intérêts légitimes », sans

donc, que le consentement de l'usager soit nécessaire. Or une telle modification ne résoudra pas les problèmes que pose, en l'occurrence, la base légale des « intérêts légitimes ». Pour invoquer celle-ci, il faut vérifier que trois conditions sont satisfaites : que l'intérêt poursuivi est bien légitime ; que le traitement des données envisagé est nécessaire et que les intérêts du responsable du traitement ne créent pas de déséquilibre au détriment des droits et intérêts des personnes dont les données sont traitées. Or la rédaction proposée ne définit pas quand ces conditions seront satisfaites. Son applicabilité est donc douteuse ; c'est au juge qu'il reviendrait de trancher. Ici encore, le texte proposé par la Commission européenne est d'une piètre qualité juridique.

L'approche adoptée pour l'AI Act et le RGPD est très médiocre d'un point de vue juridique. En effet, ce que le législateur européen appelle « approche fondée sur l'analyse des risques » implique de confier aux entreprises elles-mêmes l'évaluation des risques. Elles sont ainsi comme des enfants dans un magasin de bonbon, qu'on autoriserait à définir combien de sucre il est souhaitable et raisonnable de consommer. De telles normes juridiques ne sont pas applicables ; elles n'aident personne. Les avocats les critiquent beaucoup car elles leur rendent difficile d'indiquer à leur client ce qui est autorisé et ce qui est interdit.

J'aime dire que ces lois numériques européennes sont comme les autoroutes allemandes, où chaque conducteur définit librement sa vitesse, c'est-à-dire le niveau de risque qu'il estime correct pour lui. Mais on pourrait choisir une autre approche de l'analyse du risque, ce que font, d'ailleurs, la majorité des pays européens, en limitant la vitesse – à 30 kilomètres à l'heure devant les écoles, 50 kilomètres à l'heure en ville, et ainsi de suite. Ces limitations rendent le risque gérable, avec des lignes rouges claires.

Les conservateurs, en particulier, défendent le choix de confier l'évaluation du risque aux acteurs économiques par le souci de s'adapter aux petites et moyennes entreprises. Mais ma mère a une petite entreprise de dix employés et elle ne veut pas avoir à définir elle-même les obligations auxquelles elle doit se soumettre dès lors que le nombre d'abonnés à sa newsletter dépasse les 10 000. Dans une société démocratique, le législateur a le devoir de fixer des règles claires de régulation du numérique – ce qui est bien autre chose que de se décharger de l'évaluation du risque et de la fixation des règles sur les acteurs économiques.

Concernant votre dernière question, nous n'avons pas de preuve que les lobbys aient exercé des pressions concernant des articles spécifiques. Des rumeurs circulent, selon lesquelles certaines entreprises auraient soumis des propositions de rédaction de certains articles, mais je ne veux pas relayer de rumeurs en public.

Selon nous, le principal problème est que l'unité de la Commission européenne chargée de rédiger les propositions de directive ne dispose tout simplement pas du personnel et de l'expertise nécessaires. C'est très regrettable. Même si je ne partageais pas forcément les options politiques de l'équipe précédente, en tant qu'avocat, force est de constater qu'elle était beaucoup plus compétente. L'équipe actuelle, elle, n'est pas forcément en mesure de produire des textes juridiquement valables – les acteurs économiques eux-mêmes hésitent à souscrire à ses propositions, car ils ne voient pas bien comment elles pourraient fonctionner en pratique.

En réalité, ceux qui bénéficient des approches « fondées sur l'analyse des risques » et de la mauvaise rédaction du droit européen, ce sont les entreprises de la Big Tech, car elles disposent des services de puissants cabinets d'avocats, qui sont capables d'engager des débats interminables avec le régulateur sur le sens de chaque terme.

On entend souvent que les lois les plus flexibles sont plus adaptées aux petites et moyennes entreprises ; en réalité, elles les accablent, parce qu'elles les contraignent à recruter des avocats simplement pour comprendre à quelles obligations elles sont soumises, alors qu'elles n'en ont pas les moyens. Nous le constatons au quotidien dans les litiges : les entreprises qui gagnent à la flexibilité du droit sont celles de la Big Tech, dont les avocats débattent pendant des centaines d'heures sur les obligations légales attachées au moindre cookie. Plutôt que de se demander quel gros titre on pourra tirer d'une législation, il faut se demander à qui elle profitera réellement.

M. le président Philippe Latombe. En vertu du système de « guichet unique » du RGPD, c'est l'autorité de protection des données de l'État membre où une société est enregistrée qui est compétente pour les actions visant celle-ci – ainsi de l'autorité irlandaise pour les sociétés américaines. Or le paquet omnibus numérique tend à intégrer les règles de la directive ePrivacy dans le RGPD, et donc à renforcer les compétences des autorités nationales de protection des données. Quel bilan tirez-vous de l'action de régulation de l'autorité irlandaise ?

M. Max Schrems. C'est une vaste question. En Europe, il faut compter avec les exécutifs nationaux ; c'est d'ailleurs au niveau national que le droit européen est transposé. Or deux États membres, l'Irlande et le Luxembourg, créent des failles de plus en plus nombreuses dans le droit européen – pas seulement en matière de droit du numérique, mais aussi en matière de fiscalité et de droits sociaux.

Sans parler des entreprises de la Big Tech, la majorité des entreprises étrangères – les entreprises chinoises, par exemple – sont domiciliées dans ces deux États. Par exemple, nous avons constaté qu'une entreprise chinoise partageait une boîte aux lettres irlandaise avec 600 autres entreprises. Cela suffit pour établir que son siège est irlandais et pour la soustraire à toute poursuite des autorités françaises ou autrichiennes. Il faut faire quelque chose contre ces pratiques abusives et absurdes. Nous en sommes à un point où de nombreux choix procéduraux du régulateur irlandais relèveraient, en Autriche, de l'abus de pouvoir et constitueraient donc des infractions pénales. Pour le dire très simplement, les procédés employés en Irlande seraient, en Autriche, susceptibles d'envoyer le régulateur en prison en Autriche !

Notons que l'ancienne directrice de la Commission de la protection des données irlandaise, la DPC (*Data Protection Commission*) a récemment annoncé son embauche par le cabinet d'avocat qui défend Meta. Elle rejoint donc littéralement l'entreprise qui conteste ses propres décisions devant les tribunaux irlandais. Cela illustre une pratique que l'Irlande maîtrise assez bien, à savoir présenter une belle façade tout en expliquant qu'il lui est malheureusement impossible de faire appliquer les décisions – il me semble que, dans le cas de Meta, une des amendes dépassait 1,2 milliard d'euros. Ainsi, aucune des peines d'amende dont vous entendez parler dans la presse n'est jamais appliquée : un média public irlandais a estimé que seulement 0,3 % des montants dus ont réellement été payés, parce que toutes ces affaires restent pendantes pendant des années, du fait du régulateur comme des entreprises.

Les procédures judiciaires irlandaises sont en effet extrêmement longues, complexes et onéreuses, au point qu'un citoyen lambda n'a aucune chance de faire valoir ses droits. Même des demandes très simples, comme celle d'accéder à un dossier ou d'être entendu dans le cadre de la procédure, peuvent être refusées. Elles coûtent de toute façon au moins 100 000 euros : si, en tant que citoyen français, votre cas est transféré en Irlande, vous avez théoriquement la possibilité de poursuivre le régulateur irlandais pour son inaction, mais votre démarche n'a en réalité aucune chance d'aboutir si vous n'avez pas au moins 100 000 euros sur votre compte en banque. À l'issue de l'affaire Schrems II – j'étais alors poursuivi par le régulateur –, les frais juridiques se sont

établis à environ 10 millions d'euros. Si j'avais perdu, j'en aurais été personnellement redevable et j'aurais été déclaré en faillite. Il se trouve que j'avais raison d'accuser le régulateur de ne pas avoir fait son travail et que j'ai gagné, mais la plupart des gens ne prendraient pas un tel risque. De ce fait, si le régulateur et le système judiciaire existent sur le papier, ils sont dans les faits inaccessibles aux citoyens lambdas et ne produisent aucun résultat.

Pour en venir aux éventuelles solutions, une des pistes évoquées consiste à transférer certaines de ces fonctions de régulation au niveau européen, au moins pour les grandes entreprises. L'Europe est déjà dotée d'un Contrôleur européen de la protection des données, compétent pour les institutions européennes comme la Commission européenne. Il serait donc possible de décider que les Vlops (*Very Large Online Platforms*, les très grandes plateformes en ligne) ne doivent plus être régies par les régulateurs irlandais ou luxembourgeois mais par les institutions européennes. Cela supposerait que ces dernières se montrent à la hauteur de la tâche, ce qui n'a rien d'évident, mais nous échapperions au moins aux approches nationales qui consistent tout simplement à refuser d'appliquer la loi au nom de l'attractivité économique – car c'est bien ce qui est en jeu pour ces pays, au fond : attirer ces entreprises chez eux.

Mme Cyrielle Chatelain, rapporteure. Il y a environ quinze ans, vous avez obtenu que Facebook vous transmette les données personnelles en sa possession qui vous concernaient. Qu'avez-vous découvert ? Les choses se sont-elles aggravées depuis ? Quels types de données ces entreprises peuvent-elles désormais collecter ?

Vous avez évoqué le risque de transferts massifs de données vers les États-Unis. La question de la souveraineté et de la protection des données s'est imposée dans le débat public et de grandes compagnies comme AWS (Amazon Web Services) ou Microsoft affirment proposer des solutions souveraines. Pouvons-nous croire qu'il est possible d'utiliser ces technologies sans que nos données soient captées par ces grands groupes ?

M. Max Schrems. Votre première question renvoie au droit d'accès de la personne concernée, qui est défini à l'article 15 du RGPD. Celui-ci aussi est menacé par les réformes envisagées dans le paquet omnibus numérique. Dans le monde du travail, par exemple, il arrive que des personnes demandent à obtenir le registre des heures qu'elles ont travaillées en vue de se faire payer leurs heures supplémentaires ; elles invoquent alors cet article 15. Or, en Allemagne, on entend monter la volonté que de telles requêtes ne puissent être faites qu'à des fins de protection des données personnelles. Les entreprises, si elles pouvaient ainsi statuer sur la recevabilité de chaque demande en fonction de ses motifs, en profiteraient pour les rejeter – ce qui serait le point de départ de procédures judiciaires longues de plusieurs années. Je ne connais pas la position française sur ce point – je ne pense pas qu'il en existe une à l'heure actuelle –, mais en tout cas, l'outil dont nous disposons pour connaître l'usage qui est fait de nos données est lui aussi menacé.

Lorsque j'ai commencé mes démarches, l'argument qui m'était opposé était que, dès lors que les données étaient uniquement exploitées à des fins publicitaires, leur utilisation n'avait aucun impact, aucune conséquence sur ma vie. Sur ce point, la situation a drastiquement changé avec l'arrivée de l'IA. À ma connaissance, Meta a d'ailleurs été la première entreprise à se positionner publiquement sur ce sujet et à annoncer qu'elle utiliserait l'ensemble des données recueillies sur ses réseaux sociaux pour alimenter son modèle d'IA.

On entend souvent dire que le RGPD n'a pas prévu ces développements et qu'il est donc nécessaire d'adapter la loi à ces nouvelles technologies. Or, les vieux hommes blancs qui, en 1981, ont établi les principes qui structurent le RGPD, évoquaient déjà la possibilité que,

dans le futur, les données personnelles soient réutilisées de diverses façons alors inconnues et servent à alimenter de gros algorithmes qui prendraient des décisions étranges, dont plus personne ne serait en mesure de comprendre l'origine. C'est exactement pour cette raison que nous avons le droit d'accéder aux données collectées, de les faire supprimer ou de faire corriger de fausses informations : le sentiment dominant, à l'époque, était déjà que ces algorithmes étaient susceptibles de produire des erreurs. Nous y sommes : aujourd'hui, on appelle ces fausses informations des « hallucinations » et on constate que les données recueillies pour alimenter des IA ou des LLM (*Large Language Models*, ou grands modèles de langage) sont rassemblées dans de grands réservoirs sans qu'on sache ce qu'elles y deviennent. Une partie importante du RGPD a été rédigée précisément pour gérer ces situations.

Or, quand l'IA est arrivée, nous avons constaté que tous les régulateurs européens, y compris la Cnil (Commission nationale de l'informatique et des libertés) – qui était habituellement un régulateur très fort sur bien des sujets – ont cédé, estimant qu'il fallait tout autoriser, de peur de prendre du retard dans ce secteur. De ce fait, nous faisons maintenant face à un tsunami qui aspire toutes les données et les utilise à des fins que nous ne pouvons pas contrôler, et que les entreprises elles-mêmes ne peuvent pas contrôler. Une de nos affaires en cours concerne par exemple un ressortissant norvégien dont l'intelligence artificielle d'OpenAI prétend qu'il a assassiné ses enfants, maltraité sa femme et commis toute une série d'actes aussi horribles que fictifs. Or, quand nous demandons à OpenAI de corriger ces informations produites par son algorithme, l'entreprise explique être techniquement incapable de le faire. De nombreuses personnes témoignent de cas similaires. Il s'agit souvent de journalistes qui, parce que leur nom apparaît en tête d'articles qu'ils ont consacrés à des affaires criminelles, sont mêlés par l'IA avec le contenu desdits articles et se retrouvent ainsi accusés d'avoir tué des dizaines d'enfants ou d'avoir commis des agressions sexuelles. Que des compagnies de la Big Tech, qui engrangent des milliards, affirment n'avoir aucun moyen de corriger ces erreurs ou de traiter le problème est affligeant. C'est précisément pour ces raisons que nous nous sommes dotés des principes qui figurent dans le RGPD.

Ainsi, alors qu'on nous assurait à l'origine que les données n'étaient collectées qu'à des fins publicitaires, nous voyons bien ce qu'il en est réellement des années plus tard. Je ne crois pas que ce soit nécessairement de la mauvaise foi ni que le but réel ait toujours été celui-là, mais le fait est que c'est bien ainsi que les choses se passent.

Pour ce qui est des solutions souveraines, le nouveau terme à la mode dans le monde de la protection de la vie privée est ce qu'on appelle le *soveregnity washing*, c'est-à-dire le fait de prétendre qu'une solution est souveraine quand, en réalité, on se contente d'utiliser un bon vieux serveur américain en le parant d'un drapeau européen. C'est ce que font la plupart des entreprises de la Big Tech, pour des raisons diverses. À les entendre, agir autrement serait impossible, principalement en raison des coûts qu'induiraient les investissements nécessaires ou la mobilisation d'équipes européennes pour gérer en permanence des systèmes complètement distincts. Il est intéressant de noter que ces mêmes entreprises sont en revanche capables de proposer des solutions souveraines, ou au moins partiellement souveraines, en Chine : dès lors qu'un pays s'attache à faire réellement appliquer ses lois, la souveraineté n'est plus un problème.

Lorsqu'on échange avec ces acteurs de manière officieuse, ils expliquent surtout que le déploiement de telles solutions coûterait trop cher et que, tant que les clients ne partent pas, il est plus simple d'ignorer la loi tout en faisant un peu de relations publiques. Depuis la réélection de Donald Trump, néanmoins, les gens deviennent plus critiques et ne croient plus aussi facilement à ces effets de communication. Il me semble qu'il y a là une tendance et que,

d'ici cinq ou dix ans – cela ne pourra pas se faire du jour au lendemain –, de plus en plus d'infrastructures critiques et d'entreprises européennes opteront pour des clouds européens.

Une autre option serait de séparer complètement les services américains et européens. On pourrait par exemple imaginer une société par actions dans laquelle le propriétaire américain détiendrait seulement les actions, mais aucun droit de donner des ordres au dirigeant. Ce fonctionnement existe déjà en Allemagne ou en Autriche, ainsi que, j'imagine, dans d'autres pays. Toutefois, cela supposerait de restructurer les entreprises concernées et impliquerait donc des coûts. Or celles-ci ne voient pas l'intérêt des investissements, dès lors que les gens ne se détournent pas de leurs services et qu'elles peuvent continuer à les vendre. Toutefois certaines entreprises plus sérieuses font exception, et plus généralement, je crois que les compagnies américaines prennent conscience que, tôt ou tard, elles seront contraintes d'aller dans cette direction.

M. le président Philippe Latombe. Pendant très longtemps, la Cour de justice de l'Union européenne (CJUE) a étendu la définition des données personnelles et accru leur protection en élargissant le champ des données considérées comme sensibles. À cet égard, la décision SRB (*Single Regulation Board*, ou Conseil de résolution unique) de septembre 2025 a constitué un tremblement de terre. Comment interprétez-vous cet arrêt ? Constitue-t-il un vrai changement jurisprudentiel ou sa portée doit-elle encore être clarifiée – même s'il a servi de base à la nouvelle définition des données personnelles dans le paquet omnibus numérique ?

La CJUE est-elle la véritable instance européenne de protection des données, celle qui fixe le tempo et qui donne le la ?

M. Max Schrems. Pour répondre à votre seconde question, nous estimons que la CJUE est probablement notre seul espoir actuellement. Dans l'univers de la protection de la vie privée, le simple fait de connaître la loi et de vouloir la faire appliquer suffit pour être considéré comme un activiste, car 99 % des personnes qui travaillent dans ce domaine sont employées par l'industrie. La plupart des professeurs, par exemple, sont liés par divers contrats à des entreprises du secteur – pas tous, mais la plupart.

Cela les conduit à adopter des points de vue particuliers sur des décisions comme l'arrêt SRB. En Allemagne et en Autriche, et peut-être dans une moindre mesure en France, la littérature juridique revêt une grande importance : les tribunaux la consultent et la suivent. Or cette littérature est presque toujours rédigée par des avocats d'entreprises. Si une décision a plusieurs interprétations possibles, les ouvrages juridiques mettront en avant, dans la plupart des juridictions, une interprétation très favorable à l'industrie. En Allemagne, par exemple, les publications sont très nombreuses ; quelques-unes sont réputées pour être académiques, mais d'autres peuvent être considérées comme pratiquant un activisme pro-industrie – pour retourner l'emploi de ce terme.

Cela a une influence énorme. La CJUE y a jusqu'à présent résisté, mais elle n'est pas déconnectée de ceux qui contribuent à ce débat. L'arrêt SRB en est un premier signe. Il me semble qu'il n'a pas été bien présenté par le Contrôleur européen de la protection des données, qui s'est montré très formaliste dans son approche. Ce que nous constatons, c'est un phénomène d'écho entre les décisions des tribunaux et les vues de ceux qui composent la bulle juridique.

Dans l'arrêt SRB, la CJUE a pris le soin de reprendre explicitement tous les arrêts précédents et d'affirmer très clairement qu'elle ne modifiait pas son raisonnement juridique ; elle ne l'aurait pas fait si elle n'avait pas voulu signifier qu'elle s'en tenait à sa ligne habituelle. En l'occurrence, l'affaire portait sur le cas très spécifique de l'entreprise Deloitte, qui, pendant

deux mois, avait recueilli des données partiellement anonymisées, ou pseudonymisées. La Commission européenne et la majeure partie du secteur juridique ont extrait un ou deux demi-paragraphes du jugement pour en déduire que la définition des données personnelles avait soudain changé. Le respect dû à la CJUE imposerait pourtant de lire l'intégralité de la décision et de restituer fidèlement ce qu'elle voulait dire. On peut concevoir que, dans le cas où un destinataire unique reçoit, pendant une période limitée, des données dont on peut raisonnablement considérer qu'elles ne peuvent pas être rattachées à une personne identifiée, ces données ne sont pas des données personnelles au sens où la Cour l'entend. Mais c'est très différent de ce que la Commission européenne entend introduire dans le paquet omnibus numérique pour modifier le premier alinéa de l'article 4 du RGPD – puisque, je le répète, on pourrait conclure de cette modification que les données des utilisateurs exploitées pour la publicité en ligne ne seront plus protégées en tant que données personnelles.

En vérité, alors que l'arrêt SRB n'introduit dans la jurisprudence qu'une légère inflexion, modeste et contenue, la majorité des acteurs du secteur lui donnent un poids très lourd – c'est surtout le cas des juristes spécialisés dans ce domaine, qui cherchent avant tout à vendre une solution magique. De nombreux clients seraient prêts à payer 20 000 euros pour obtenir un bout de papier leur signifiant que le RGPD ne s'impose plus à eux : ils savent que cela n'arrivera probablement jamais, mais, pour cinq ans, ils pourront faire ce qu'ils veulent, en attendant que les régulateurs réagissent. Pour un dirigeant d'entreprise, le fait qu'un cabinet d'avocats lui assure que, à la lumière du jugement SRB, ses actions sont parfaitement légales est un parfait chèque en blanc. Je crois que, si on creuse un peu, c'est ce qu'il se passe. Mais les gros titres de la presse reflètent le plus souvent les opinions de ces juristes, et non celles des autorités de protection des données.

Mme Cyrielle Chatelain, rapporteure. Voilà des années que vous utilisez le droit pour combattre les géants du numérique. Croyez-vous toujours que la loi est le bon outil, ou en tout cas qu'elle est un outil nécessaire, pour mener cette lutte ? Si oui, quelles mesures pourrait-on prendre pour gagner en rapidité et en efficacité, et peut-être pour équilibrer le rapport de force entre les multinationales et les citoyens ?

M. Max Schrems. C'est une question difficile. Lorsque vous vous engagez dans ces procédures – et nous en avons plus de 800 en cours – et que vous comprenez que le délai moyen ne serait-ce que pour accéder à vos données est de cinq ans en Europe, vous vous demandez nécessairement si l'État de droit par lequel nous sommes théoriquement régis bénéficie réellement aux citoyens. Cela dit, il n'existe pas d'alternative à l'État de droit.

Il me semble qu'il nous faut changer de psychologie, changer la façon dont nous percevons les entreprises de la Big Tech. En Autriche, l'entreprise Temu a violé une multitude de dispositions du droit du travail. Le gouvernement a décidé de poster des policiers devant ses locaux et de demander à chaque salarié de présenter son permis de conduire et ses papiers d'identité ; il s'est trouvé que la plupart n'en avaient pas. De la même façon, en matière numérique, les autorités publiques doivent regagner du terrain. Nous en sommes venus à croire que ces sociétés sont au-dessus des lois – comme si elles flottaient dans leurs propres clouds, en quelque sorte –, mais, en réalité, ce sont de vraies entreprises, avec de vrais comptes en banque et elles sont redevables devant des juridictions.

C'est une question de culture. Un jour, le responsable d'une autorité de protection des données est venu me voir à l'issue d'une conférence pour me dire combien ce serait drôle si les mesures que j'avais exposées étaient mises en œuvre. Quand on songe qu'il s'agissait précisément des lois qu'il était chargé de faire appliquer, c'est ahurissant ! C'est comme si une

agence de lutte contre la drogue déclarait : « Ce serait drôle de faire quelque chose pour empêcher le trafic de cocaïne, non ? » Telle est la réalité avec laquelle nous devons composer sur le terrain. Le RGPD est souvent présenté, à tort, à l'opinion publique comme une législation horrible, impossible à mettre en œuvre. Il est vrai que les chiffres disponibles à l'échelle européenne montrent que moins de 1,3 % des plaintes débouchent sur une amende. En Autriche, seules soixante-six amendes sont prononcées chaque année ; dans le même temps, les autorités viennoises ont été capables de verbaliser plus de 1000 trottinettes électriques ers mal garées en un mois l'été dernier ! Tout dépend des priorités que nous nous fixons.

J'ajouterai que, d'un point de vue financier, le gouvernement aurait beaucoup à gagner à faire appliquer la loi. J'ai par exemple fait remarquer au gouvernement autrichien qu'une seule amende infligée à Google lui permettrait de financer le tunnel de base du Brenner, qui doit relier l'Autriche à l'Italie. Ce laisser-faire dans le domaine de la protection de données reflète davantage la culture des régulateurs et des spécialistes du sujet que la lettre de la loi.

Quant à ce que nous pouvons faire, il existe en Europe une procédure de recours collectif, comparable aux *class actions* (actions de groupe). Je ne suis pas très partisan de ces procédures, car elles visent à réparer les dommages une fois qu'ils ont été commis alors que la régulation devrait idéalement permettre de les prévenir, mais elles auraient au moins le mérite de faire en sorte que les entreprises américaines qui violent nos lois en subissent les conséquences.

Les États membres auraient aussi pu se saisir de l'alinéa 2 de l'article 80 du RGPD, qui autorise les ONG comme la nôtre à lancer des actions collectives. Aucun ne l'a fait, alors que cette clause nous aurait permis de porter devant la justice de nombreuses affaires que nous ne parvenons pas à faire aboutir. À titre d'exemple, nous recevons de nombreuses plaintes de parents qui nous demandent d'agir contre les atteintes à la vie privée subies par leur enfant, mais aucun d'eux n'accepte que celui-ci soit identifié comme plaignant dans une procédure officielle – contre l'école ou une autre institution –, précisément par crainte de nuire à sa vie privée. L'alinéa 2 de l'article 80 nous permettrait de traiter des situations de ce type.

Un autre élément important concerne le délai maximal dont l'État dispose pour prendre une décision. En Autriche, par exemple, si le régulateur n'a pas agi dans un délai de six mois, le plaignant peut saisir les tribunaux. En Irlande, aucun délai ne s'applique : une attente de cinq ans peut être considérée comme raisonnable et le plaignant peut être amené à payer les frais de justice à l'issue de la procédure.

De nombreuses spécificités nationales pourraient ainsi être modifiées pour faciliter concrètement notre travail – mais l'amélioration des procédures est un sujet extrêmement ennuyeux, donc peu susceptible de faire les gros titres de la presse.

M. le président Philippe Latombe. Merci de vous être rendu disponible pour répondre à nos questions et merci pour tout ce que vous faites pour la protection des données. Nous suivrons avec attention les actions de votre association. Peut-être pourrons-nous vous transmettre nos conclusions en amont de leur publication, pour que vous puissiez nous dire si elles vous semblent utiles et réalistes.

La séance s'achève à douze heures vingt-cinq.

Membres présents ou excusés

Présents. – M. Nicolas Bonnet, Mme Cyrielle Chatelain, M. Philippe Latombe, M. Vincent Thiébaut

Excusés. – M. Philippe Gosselin, M. Alexandre Sabatou