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

Mercredi
25 mars 2026
Séance de 17 heures

Compte rendu n° 10

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-sept heures cinq.

M. le président Philippe Latombe. J'ai le plaisir d'accueillir Mme Meredith Whittaker, présidente de la Signal Foundation, à l'origine de la messagerie Signal, qui a auparavant exercé des fonctions au sein de Google ainsi qu'à la Federal Trade Commission.

L'application de messagerie Signal place au cœur de son projet la préservation de la confidentialité de ses utilisateurs. Pourriez-vous, à cet égard, nous exposer ses spécificités par rapport à d'autres applications commerciales équivalentes en matière de protection de la vie privée ? Je vais vous laisser la parole pour une présentation liminaire, à l'issue de laquelle nous pourrons engager un échange sous forme de questions-réponses.

Mme Meredith Whittaker, présidente de la fondation Signal. Je vous remercie de m'offrir l'opportunité d'aborder les questions de la vie privée, de la souveraineté numérique, des vulnérabilités systémiques de notre paysage technologique actuel, et de l'importance cruciale de pouvoir vérifier les infrastructures qui sous-tendent nos vies et nos institutions.

Comme vous le savez, notre époque se caractérise notamment par une concentration industrielle d'une ampleur inédite. Il n'est pas nécessaire de vous convaincre, tant vous êtes déjà sensibilisés à cette question, qu'elle ne relève pas du seul domaine économique. Une telle concentration constitue également une vulnérabilité géopolitique et compromet notre capacité à gouverner, à nous reconstruire et à protéger nos États, ainsi que nos relations sociales et économiques. Face à ces enjeux particulièrement graves, il nous appartient d'abord de comprendre les mécanismes qui nous ont conduits à cette situation. Je consacrerai ainsi quelques instants à présenter le modèle économique fondé sur la publicité et la surveillance, à l'origine de l'extrême concentration que nous observons aujourd'hui.

Ce problème a été façonné par les dogmes néolibéraux des années 1980 et 1990, qui postulaient que la privatisation relevait de la volonté divine, que les marchés étaient bienveillants et que contrôler leur croissance serait une perversion. Ce contexte a préparé le terrain pour la concentration du contrôle d'infrastructures clés comme Amazon Web Services (AWS), Microsoft Azure, Google cloud, les plateformes d'information des réseaux sociaux comme X et YouTube, et les systèmes de prise de décision basés sur l'intelligence artificielle qui orientent les choix de nos États, de nos institutions et de nos entreprises. À Bruxelles, à Paris, comme partout dans le monde, de nombreuses analyses sont avancées pour expliquer cette situation, qu'elles invoquent un déficit d'innovation ou une insuffisance de la réglementation, mais ces interprétations passent à côté de l'essentiel. La réalité tient à ce que la privatisation d'internet, soutenue par l'État américain, a conduit à méconnaître les enseignements de l'histoire ainsi que la nature même des réseaux de communication, depuis la poste et le télégraphe jusqu'aux télécommunications. Il était logique, jusqu'à ce que nous l'oubliions, de considérer ces dernières comme des monopoles naturels puisqu'en raison de facteurs tels que les économies d'échelle, le coût très élevé des actifs, les effets de réseau et d'autres tendances centralisatrices, il n'existe pas de moyen pratique de créer des concurrents. Personne ne souhaiterait disposer de dix-huit téléphones différents, chacun relié à un groupe d'amis distinct. Cette réalité ainsi que l'importance critique de l'information, de la communication, des flux d'actualités et des chaînes de commandement militaires explique que, historiquement, les réseaux aient été constitués en monopoles réglementés. Ce n'est d'ailleurs pas sans raison que la communication figure parmi les cibles prioritaires en temps de conflit car, en son absence, plus rien ne fonctionne.

Pourtant, traiter les réseaux comme des monopoles naturels n'a pas été le choix de l'administration Clinton dans les années 1990, lorsque les règles de la commercialisation d'internet ont été écrites. Ces règles ont donné la priorité aux entreprises américaines et ont livré internet aux forces du marché. L'accent mis sur l'avantage des entreprises américaines, qui ont été les premières sur le marché grâce aux investissements dans l'infrastructure aux États-Unis et à la puissance du *soft power* américain, permettent d'expliquer cette hyperconcentration de géants de la technologie aux États-Unis et, dans une moindre mesure, en Chine. La Chine est en effet le seul État doté d'un marché intérieur suffisant pour soutenir de telles alternatives, et elle a délibérément exclu la technologie américaine. C'est pourquoi, quels que soient les milliards mis de côté ou la fréquence à laquelle on évoque les giga-usines, il n'est pas possible de faire émerger de nouveaux entrants sur ce marché, étant donné les conditions établies par ces géants.

Je le redis, si nous nous trouvons aujourd'hui dans cette situation, ce n'est ni en raison d'une réglementation excessive, ni parce que l'innovation ne ferait pas partie de la mentalité française, ni encore faute d'une union des marchés de capitaux, mais parce que le monopole et les décennies d'avance accumulées par les entreprises américaines nous ont conduits au point où nous sommes désormais. Telle est la situation que nous devons examiner ensemble. Cette réalité est certes difficile à admettre, mais il serait plus grave encore de la nier ou de s'y soustraire. Il nous appartient de l'affronter sans peur, car c'est ainsi que nous gagnons en clarté, que nous comprenons mieux le paysage et que, en ajustant notre regard, nous discernons des fissures dans cette forteresse prétendument impénétrable.

J'entends par là qu'il subsiste encore de l'espoir. De nombreuses choses échappent aux capacités actuelles des entreprises de la tech et de l'IA, alors même qu'elles sont indispensables à nos économies, à nos systèmes financiers, à nos armées, à nos institutions de défense et au fonctionnement de nos démocraties. Même si les questions éthiques sont indispensables, les plateformes n'apportent pas ces garanties. Je souhaiterais donc énumérer quelques opportunités qui s'offrent à nous afin de repartir sur des bases plus saines, en nous appuyant sur des règles que nous définissons nous-mêmes plutôt que sur les récits de ceux qui, forts de leur puissance, s'emploient à préserver à tout prix leur position dominante. Il existe en effet de multiples manières de concevoir la technologie, comme en témoigne Signal, et nous avons besoin de nombreuses technologies dont nous ne disposons pas encore. À cet égard, il est impératif d'accorder une attention bien plus grande aux vulnérabilités des modèles d'intelligence artificielle et des systèmes qui les mobilisent, qu'il s'agisse de l'empoisonnement des données, de l'exfiltration ou d'autres attaques largement documentées pour lesquelles il n'existe à ce jour aucun remède. Seule une compréhension lucide de cette réalité permettra de dégager des solutions et de veiller à ce que les systèmes intégrés à nos infrastructures ne deviennent pas des vecteurs de dommages significatifs.

Parallèlement, il nous faut investir dans le développement sécurisé ainsi que dans des chaînes d'approvisionnement pour les données et d'autres processus qui ne s'inscrivent pas dans l'approche des grandes entreprises de l'IA, pour lesquelles « *plus c'est gros, mieux c'est* », tout en gardant à l'esprit les fondamentaux de la technologie : l'IA n'a rien de magique, elle n'est pas une divinité, pas davantage un ami ou un amant et, à l'instar de tout système composé de matériel et de logiciels assorti de dépendances logicielles, elle doit être sécurisée au moyen de bonnes pratiques de développement. Or tel n'est pas le cas aujourd'hui, notamment dans le contexte de l'IA agentique, et cela constitue à la fois un avertissement et une opportunité de tenir bon.

Il nous appartient ainsi de veiller à ce que la séparation entre les systèmes d'exploitation et la couche applicative, par exemple entre un agent IA et vos messages Signal, ne soit pas remise en cause par un déploiement hasardeux de l'IA. Il convient également de rappeler qu'il n'existe aucune intelligence intrinsèque sans données, puisqu'un modèle d'IA ne peut connaître que ce qui relève de la distribution des données sur lesquelles il a été entraîné, d'où la nécessité de disposer de données beaucoup plus robustes, qu'il s'agisse de données scientifiques destinées à la recherche fondamentale ou de données élaborées avec une attention particulière afin de garantir une rigueur méthodologique adaptée à la défense, à la santé ou à certains secteurs industriels, ce qui constitue également une ouverture de marché. Enfin, il importe de souligner la nécessité de modifier les règles du jeu, dans la mesure où les entreprises en place façonnent un monde conforme à leurs intérêts où les modalités d'évaluation des systèmes ne reflètent pas leurs usages réels. Cette situation doit être envisagée, là encore, comme une opportunité de définir des critères de valorisation prenant pour référence la réalité des usages et mesurant la performance de l'IA dans le monde réel, plutôt qu'au regard d'un étalon abstrait, ce qui permettrait de constater que des modèles souvent plus modestes offrent les meilleures performances tout en réduisant notre dépendance à l'égard des *hyperscalers*.

Cette liste demeure nécessairement partielle et trop brève, tant chacun de ces points pourrait donner lieu à de multiples développements. Il s'agissait simplement d'offrir un aperçu des trajectoires possibles pour progresser. Puissions-nous, en nous affranchissant de ce sentiment d'insécurité, adopter une réflexion créative sur la manière de construire ce dont nous avons véritablement besoin, car il existe une pluralité d'usages de la technologie, une diversité d'approches et de modes de financement, et il est impératif de ne pas dépendre des leaders actuels de la technologie et du monde.

M. le président Philippe Latombe. Lors de votre venue en France, il y a un an et demi, nous débattions à l'Assemblée de l'affaiblissement du chiffrement, et vous aviez alors adopté une position très claire en indiquant que, si la France devait imposer une telle mesure, vous envisageriez de rendre Signal indisponible sur le territoire national. Si je reformule la question sous un autre angle, imaginons que la Maison-Blanche vous demande aujourd'hui de ne plus rendre Signal accessible en France : accepteriez-vous une telle injonction ? Et, dans l'hypothèse où vous décideriez de ne pas vous y conformer, quelles en seraient les conséquences juridiques pour la Fondation Signal ?

Mme Meredith Whittaker. Je préfère m'abstenir de toute spéculation basée sur des hypothèses, dans un contexte géopolitique particulièrement instable et au regard de la multiplicité des enjeux en présence. Ce que je peux en revanche affirmer, c'est que nous irons très loin pour garantir que Signal demeure accessible à tous, partout. Quelle que soit la juridiction concernée, nous sommes prêts à ne pas nous conformer à des injonctions qui seraient contraires à notre mission ainsi qu'à l'intégrité technologique qui en constitue le fondement.

Mme Cyrielle Chatelain, rapporteure de la 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. Pourriez-vous présenter, à l'attention de celles et ceux qui ne le connaissent pas, le modèle de Signal ainsi que l'attention particulière qu'il accorde à la protection des données personnelles, et en expliquer l'importance ?

Pourriez-vous également préciser en quoi le modèle de la fondation, en tant que modèle économique spécifique, permet précisément de ne pas monétiser les données ?

Enfin, dans le prolongement de cette interrogation, vous étiez effectivement venue évoquer l'affaiblissement du chiffrement. Êtes-vous aujourd'hui préoccupée par les évolutions en Europe, qu'il s'agisse du projet Chat Control ou d'autres initiatives nationales visant à affaiblir le chiffrement ?

Mme Meredith Whittaker. Signal est la plus grande plateforme de communication privée. Notre seul et unique objectif est de fournir un moyen de communiquer de manière réellement privée dans un monde où une part croissante de nos vies se trouve placée sous la surveillance de grandes entreprises technologiques. Pour nous, la communication privée est un droit humain fondamental, sans lequel la démocratie et une vie pleine de sens ne sont pas possibles. Nous existons pour protéger ce droit et nous le faisons en fournissant un outil, un logiciel et des protocoles open source qui sont essentiels à la protection de la vie privée. Le protocole de Signal est le standard pour le chiffrement des messageries. Lorsque nous l'avons introduit en 2013, il a représenté une avancée majeure dans les pratiques de chiffrement et la cryptographie appliquée. Il est utilisé non seulement par Signal, mais également par d'autres acteurs sous licence pour protéger la confidentialité de leurs communications.

En plus de ce protocole qui protège le contenu des messages, nous faisons tout notre possible pour protéger les métadonnées, c'est-à-dire les informations extrêmement sensibles : à qui vous parlez, à quel moment, quelles sont vos informations de profil, qui fait partie de vos groupes de discussion, à quel moment vous avez commencé à parler à un thérapeute, contacté un avocat spécialisé en divorce ou un oncologue. Nous avons, métaphoriquement, réécrit toute notre infrastructure technologique pour nous éloigner de la norme de l'industrie, qui consiste à collecter et partager des données, afin de ne collecter que le strict minimum de données possible.

Cela répond également à la question de savoir pourquoi il n'existe qu'un seul Signal dans un monde qui a pourtant un grand besoin de technologies de ce type. Je l'ai d'ailleurs évoqué dans mon introduction : le moteur économique de l'industrie technologique repose sur la collecte de données, qui est monétisée en vendant les modèles créés par ces données. C'est ainsi que se génèrent les revenus dans un secteur dont le fonctionnement est extrêmement coûteux. Signal considère que cette norme, cet impératif économique, constitue une menace pour la mission que nous poursuivons ainsi que pour les droits que nous entendons défendre. En tant qu'organisation à but non lucratif, nous ne sommes pas soumis à cet impératif puisque nous ne disposons ni d'un conseil d'administration nous incitant à générer des profits, ni de fonds spéculatifs exigeant un retour sur investissement qui, dans cette industrie, nous conduiraient à collecter des données à des fins commerciales.

Pour autant, je peux avancer des arguments convaincants, mais cela demeure insuffisant lorsqu'il est question d'un élément aussi fondamental. La norme devrait être de pouvoir vérifier et valider par soi-même, en accédant aux fondements techniques. La confiance ne doit pas reposer uniquement sur Signal, mais sur l'ensemble des infrastructures qui la composent, car il s'agit d'un bien trop précieux pour être abandonné à l'appréciation d'un conseil d'administration ou d'un investisseur.

Nous ne sommes pas simplement open source, au sens d'un code que l'on peut consulter si l'on en a le temps. Au cours des dix dernières années, nous avons acquis, au sein de la communauté technique, une réputation qui nous place véritablement comme un étalon de référence. Cela signifie qu'un écosystème complet s'est structuré autour de nous : nous ne nous limitons pas à publier du code dans une bibliothèque en ligne, mais nous avons développé une infrastructure entière qui fonde la confiance du public, non sur des opinions, mais sur des faits.

Les hackers savent que, s'ils parviennent à compromettre notre système, ils trouveront un emploi chez nous. Ainsi, il n'est nul besoin de me croire sur parole, et tel n'est d'ailleurs pas mon objectif, car toutes les preuves sont accessibles.

M. Éric Bothorel (EPR). Je regrette tout d'abord qu'il n'y ait pas plus de monde dans cette salle pour vous entendre, à l'heure où notre Assemblée nationale évoque si souvent les sujets du numérique, de la souveraineté et du chiffrement de bout en bout.

Signal est aujourd'hui largement utilisé comme outil de communication chiffrée pour sa sécurité et sa confidentialité. Cependant, sa dépendance à des infrastructures étrangères comme AWS soulève des enjeux de souveraineté numérique pour la France et l'Europe. En tant que député, je cherche à comprendre quelles initiatives concrètes vous envisageriez pour permettre aux États et aux citoyens européens d'utiliser votre outil tout en favorisant des solutions d'hébergement local, des partenariats européens ou des architectures techniques souveraines qui garantiraient à la fois l'indépendance stratégique et la protection des données personnelles.

Par ailleurs, Signal se veut gratuit et éthique, et vous avez déjà abordé son modèle économique, mais maintenir un service sécurisé et indépendant a un coût. Quels compromis seriez-vous prêts à faire sur l'accessibilité, les fonctionnalités ou la confidentialité si le financement devenait insuffisant ?

Enfin, j'entends l'argument relatif à l'open source mais celui-ci est également avancé par certains de vos concurrents, notamment Google. Bien qu'Android soit open source, il apparaît clairement que cette caractéristique ne suffit pas, à elle seule, à garantir la transparence, l'accessibilité et le maintien en conditions opérationnelles des outils, sans contrepartie économique et dans le seul intérêt des usages des consommateurs.

Mme Meredith Whittaker. Vous affirmez, dans votre première question, qu'il ne suffit pas d'être open source, et vous avez parfaitement raison. C'est précisément pour cette raison que j'ai évoqué l'existence d'un écosystème chargé de valider et d'auditer en permanence Signal. Nous souhaiterions d'ailleurs qu'Apple permette un niveau équivalent de vérification sur iOS. Nous procédons à la vérification des dépendances afin d'identifier d'éventuelles vulnérabilités et nous nous efforçons de porter les standards au niveau le plus élevé possible. Autrement dit, si l'open source constitue le socle, il doit impérativement s'accompagner de l'ensemble des mécanismes garantissant une véritable capacité de vérification, non seulement pour Signal, mais également pour les autres infrastructures et plateformes.

S'agissant, en second lieu, de l'hypothèse dans laquelle Signal viendrait à ne plus disposer de financement, tel n'est pas le cas aujourd'hui et je n'entends pas que cela advienne car, en l'absence de financement, rien ne peut subsister. Signal occupe toutefois une position singulière puisque nous constituons une infrastructure essentielle pour des gouvernements et des armées à travers le monde, et nous sommes le principal système de communication pour toute personne ayant des informations confidentielles à partager, qu'il s'agisse de travailleurs humanitaires ou d'acteurs étatiques, précisément parce que nous représentons l'étalon de référence. Nous bénéficions en outre d'un écosystème qui, s'il était apprécié selon les critères du marché et des entreprises, vaudrait plusieurs milliards au regard de notre réputation et du rôle que nous jouons. Mon hypothèse est que nous pouvons faire en sorte que ceux qui tirent bénéfice de l'accès à cette plateforme souhaitent en assurer le financement.

Cela étant, cette perspective ne répond pas à la question de fond, qui est : comment se fait-il qu'un dispositif aussi vertueux et nécessaire que Signal ne constitue pas le modèle par défaut ? Une telle situation met en évidence un biais économique structurel et appelle d'autres interrogations, notamment sur les modalités permettant d'assurer la pérennité d'une infrastructure réellement indispensable. J'ai déjà abordé, de manière implicite dans mon introduction, la question des dépendances, qui ne sont pas substituables. Certes, il est possible d'évoquer la fédération, mais celle-ci présente également ses propres limites. Comment, par exemple, garantir une couverture mondiale pour un utilisateur en déplacement, notamment lorsqu'il part en vacances ? Cela suppose la présence de serveurs partout dans le monde afin d'éviter toute perte de données.

Dans les années 1990, les conditions ont été réunies pour permettre à un nombre restreint d'entreprises de s'imposer dans une logique de monopole et nous utilisons aujourd'hui leurs serveurs parce que cela est nécessaire pour assurer une couverture mondiale, sans disposer, pour notre part, des milliards de dollars annuels requis pour reproduire de telles infrastructures. Toutefois, nous mettons en œuvre un chiffrement rigoureux qui garantit que, même en recourant aux serveurs de ces entreprises, celles-ci ne peuvent accéder à vos données, puisque seul l'utilisateur détient les clés permettant d'accéder à ses communications sur Signal.

Mme Cyrielle Chatelain, rapporteure. Dans plusieurs de vos interventions publiques, vous avez évoqué la concentration des pouvoirs, dont la dépendance de Signal à AWS constitue une illustration. Au-delà de la question du financement, quels dispositifs conviendrait-il de mettre en place afin de déconcentrer ces pouvoirs et de ne plus dépendre d'un nombre restreint de grandes entreprises telles qu'AWS ?

Par ailleurs, dans une interview accordée au *Grand Continent*, vous mentionnez brièvement que Microsoft semble s'inscrire dans une logique de prise de contrôle. Quels sont les éléments qui vous conduisent à considérer que cette entreprise adopte une posture offensive ?

Enfin, ma troisième question porte sur des entreprises françaises ou européennes telles que Mistral AI : selon vous, l'idée de faire émerger un géant du numérique européen est-elle à la fois crédible et pertinente ?

Mme Meredith Whittaker. Comme je l'ai indiqué dans mon introduction, je ne vois pas de possibilité, à court ou à moyen terme, de répliquer les infrastructures détenues par ces monopoles. Il ne s'agit pas uniquement de l'infrastructure d'AWS, mais également d'Amazon Marketplace, des économies d'échelle, ainsi que d'entreprises ayant façonné l'écosystème au sein duquel l'ensemble fonctionne. Elles ont défini les processus, les normes, jusqu'à ce que signifie être un programmeur, et ont conçu des applications pour des environnements spécifiques, en recourant à des langages propres à ces environnements, à l'image de celui d'Apple, qui ne peut fonctionner que dans ce cadre. Ces dépendances se sont construites sur plusieurs décennies et ne sauraient être simplement reproduites, compte tenu des économies d'échelle, de la couverture mondiale et des milliards nécessaires au maintien en fonctionnement de systèmes d'une telle ampleur.

Je ne crois pas que l'objectif consiste à chercher, par quelque procédé quasi magique, à tout répliquer. J'y vois plutôt une illustration de l'échec européen, dont nous n'avons pas besoin. D'autres voies existent, comme je l'ai esquissé, qui consistent à examiner ces infrastructures et la manière dont elles peuvent nous nuire. Il convient d'apprécier ce que Signal apporte en termes de viabilité car il s'agit, en définitive, d'une question de sécurité. À cet égard,

je considère que les États-Unis devraient l'exiger, comme tous les autres États. Il y a un an, certains systèmes se sont totalement effondrés en raison d'une dépendance intégrale. Cet exemple démontre la nécessité de disposer de systèmes beaucoup plus robustes, et il me semble que les États, en leur qualité de grands clients de ces entreprises, devraient l'imposer.

Par ailleurs, des marges de manœuvre importantes existent pour tenter de faire évoluer le système. Il importe de s'intéresser à des modèles de plus petite échelle qui pourraient, en réalité, correspondre davantage aux exigences que l'on formule à l'égard de ces systèmes. Cela suppose de comprendre plus précisément ce que signifie, pour un modèle, réussir la tâche qui lui est assignée. Or il ne revient pas aux entreprises technologiques de concevoir des solutions qui ne correspondent pas nécessairement, ni de manière exacte, aux besoins exprimés par les utilisateurs.

Mme Cyrielle Chatelain, rapporteure. Je me permettrai de reposer deux questions. La première concerne votre position sur les différentes tentatives de législation qui affaiblissent le chiffrement, que ce soit par la création de portes dérobées (backdoors) ou l'initiative Chat Control au niveau européen. J'aimerais avoir votre avis sur ces législations.

La deuxième porte sur Microsoft. Une de vos paroles a été rapportée dans un journal sur une éventuelle prise de contrôle par Microsoft. Si vous le confirmez, quels sont les éléments qui vous permettent de l'affirmer ?

Ma troisième question s'inscrit dans le prolongement d'éléments que vous avez évoqués. Vous avez notamment indiqué, dans plusieurs entretiens, que Google s'était développé au détriment de certains fondamentaux en matière de sécurité, tels que la capacité à maîtriser l'empoisonnement des données. Pourriez-vous préciser ce point et nous éclairer davantage sur les failles de sécurité susceptibles d'affecter les grands groupes ? Par ailleurs, vous avez souligné la nécessité d'évaluer l'efficacité des modèles à l'aune de résultats concrets. Une étude du MIT indique que l'IA générative aurait peu, voire pas, d'impact sur le retour sur investissement pour 95 % des entreprises. Dans ce contexte, pourriez-vous préciser quels types de modèles, en particulier ces modèles de plus petite taille que vous avez évoqués, seraient susceptibles de produire des résultats nettement plus probants, tant sur le plan économique que démocratique ?

Mme Meredith Whittaker. Concernant Chat Control, ma réponse ne fera que reprendre des éléments déjà exprimés, mon appréciation n'ayant pas évolué. J'avoue éprouver une certaine lassitude à devoir revenir sur ce sujet, alors même qu'il devrait apparaître évident, pour quiconque s'intéresse à la réalité géopolitique et à ses conséquences, que l'agrégation d'un volume aussi considérable de données sous le contrôle d'entreprises relevant de juridictions américaines, et non françaises ou européennes, constitue en soi un problème. Pourtant, les tentatives visant à fragiliser les fondements mêmes de la vie privée et de la confidentialité persistent et je n'ai, pour ma part, connaissance d'aucun élément probant établissant que le chiffrement constituerait la frontière séparant les citoyens respectueux de la loi des criminels. Cette idée relève d'une construction fantasmée, qui suppose l'existence d'une autorité ou d'un acteur providentiel capable de nous protéger.

Je vais être très directe. Nous disposons des fichiers Epstein, et pourtant très peu de poursuites ont été engagées pour des préjudices considérables contre des mineurs. On va nous faire croire que dans un monde où la quantité de données de surveillance disponibles est sans précédent dans l'histoire de l'humanité, où l'accès aux données n'a jamais été aussi étendu, la difficulté à établir les faits consisterait à rechercher une aiguille dans une botte de foin parce

qu'ils sont noyés sous les données ? Serions-nous incapables d'identifier les pasteurs, les oncles ou les pères impliqués dans des abus sur des enfants ? Soit ces données n'existent pas, soit elles existent sans que la volonté de poursuivre soit au rendez-vous. Et, dans ce contexte, il serait soutenu que le chiffrement, qui constitue la seule technologie permettant d'assurer la confidentialité, serait à l'origine du problème ? Pour moi, il s'agit de « foutaises ». Cet argument est répété depuis les années 1990, alors même que le consensus technique établit qu'il n'est pas possible de modifier les lois des mathématiques afin de permettre à une seule personne d'accéder aux données. Soit le chiffrement est rompu pour tous, et les données se retrouvent alors entre les mains de ceux qui détiennent l'infrastructure, soit il fonctionne pour tous, y compris pour la personne que vous détestez le plus, faute de quoi il ne protégera pas davantage celle que vous aimez le plus. Telle est ma réponse sur la question du contrôle du chiffrement.

S'agissant de Microsoft, j'hésite à m'exprimer, dans la mesure où ma maîtrise du français ne me permet pas de conduire des entretiens dans cette langue avec toute la précision requise, de sorte que je ne suis pas certaine de ce que j'ai pu dire. Il est possible qu'une interprétation ait été faite quant à l'idée d'une volonté de contrôle total de la part de cette entreprise. Nous savons néanmoins qu'à Bruxelles, des milliers de lobbyistes agissent pour le compte de ces sociétés afin d'obtenir des avantages, et que leurs investissements en Europe sont considérables. Le terme de « souveraineté » est ainsi fréquemment mobilisé à des fins promotionnelles, plutôt que comme une notion rigoureuse renvoyant au contrôle et à l'autonomie, ce qui en constituerait une définition plus fidèle.

En ce qui concerne les processus de travail, les vulnérabilités et les chaînes d'approvisionnement, vous avez évoqué Google. Les pratiques dominantes consistent à agréger de vastes volumes de données, issues par exemple d'Alexa ou de Gmail, ainsi que des données provenant du web et de vos appareils connectés, pour les injecter dans un modèle, qui est ensuite ajusté par des travailleurs, généralement faiblement rémunérés et localisés dans les pays du Sud. Dans un tel cadre, et au regard des contraintes de coûts qui pèsent sur ces entreprises, rien n'est véritablement conçu pour préserver l'intégrité des données face à des attaques d'empoisonnement. Je ne sais pas si vous avez vu *The Manchurian Candidate*, mais cet exemple est éclairant. Une chaîne d'approvisionnement sécurisée supposerait des processus bien plus exigeants et une approche profondément renouvelée des données, de leur production à l'évaluation de leur intégrité. Il s'agit là d'un besoin manifeste et, une fois encore, d'une opportunité de marché.

S'agissant de la pluralité des approches, je souhaiterais vous répondre par écrit, car la réponse dépend étroitement des environnements considérés et nécessiterait des évaluations plus approfondies. Nous sommes confrontés à un dilemme épistémologique puisque des modèles de grande taille, réputés performants au regard d'indicateurs de référence, s'avèrent très souvent défaillants lorsqu'ils sont déployés dans des conditions réelles. Ils ne fonctionnent pas avec les données qu'ils reçoivent, ne s'intègrent pas aux infrastructures existantes (les infirmières d'un hôpital, par exemple, ne peuvent les utiliser faute d'interopérabilité avec les autres systèmes) et présentent des contraintes techniques comme une consommation excessive de mémoire vive. Autant de difficultés concrètes qui expliquent que ces grands modèles se révèlent fréquemment inopérants en situation réelle. Il est donc nécessaire de développer des méthodes d'évaluation ancrées dans le monde réel, plutôt que dans un cadre abstrait fondé sur les modèles eux-mêmes.

Enfin, il convient de souligner que ces évaluations se limitent trop souvent au seul modèle d'IA, alors même que, dans la réalité, celui-ci ne constitue qu'un élément d'un système beaucoup plus vaste, comprenant des bibliothèques logicielles, des dépendances et des conditions de déploiement, qui doivent également faire l'objet d'une analyse et d'une mesure

rigoureuses. Nous devons donc disposer de systèmes de mesure plus holistiques lorsque nous nous demandons ce qui fonctionne. Nous avons de nombreuses preuves que la réponse est souvent d'opter pour des modèles plus petits, mieux ciblés, et des déploiements plus rationnels, afin de réduire nos dépendances vis-à-vis de ces grands acteurs et de leur paradigme de la mise à l'échelle à tout prix.

M. le président Philippe Latombe. J'aurais une question en prolongement de vos propos sur l'IA et son déploiement dans les logiciels : quels sont, selon vous, les risques liés à l'intégration d'une IA agentique dans les systèmes d'exploitation ? Une telle évolution fait-elle peser des risques significatifs sur des entités critiques nationales, quelle que soit leur nationalité ? S'agit-il, à vos yeux, d'un véritable problème dès aujourd'hui ? Disposez-vous de solutions permettant d'en atténuer ou d'en contourner les effets ?

J'aurais également une question plus prospective. Vous représentez une fondation disposant d'une forte expertise en recherche cryptographique : à quel horizon situez-vous, pour votre part, l'enjeu quantique ? Comment fonctionnerons-nous avec le quantique ? Devons-nous dès à présent nous projeter dans cette nouvelle technologie et y investir, si tant est qu'il ne soit pas déjà trop tard ? Selon le calendrier de déploiement que vous anticipez pour le quantique, comment pourrions-nous procéder afin de disposer de solutions opérationnelles dans les années à venir ?

Mme Meredith Whittaker. S'agissant de l'IA agentique et de son intégration dans les systèmes d'exploitation, qu'elle soit mise en œuvre directement par les fournisseurs ou par l'intermédiaire de dispositifs qui incitent les utilisateurs à accorder à ces agents des permissions extrêmement intrusives leur ouvrant l'accès à l'ensemble de leurs données, notre inquiétude est, évidemment, très vive. Voilà en effet plusieurs années que nous exprimons nos réserves face à ces évolutions nouvelles. Nous observons en effet une pression croissante en faveur d'une intelligence artificielle appelée à exercer toujours davantage de contrôle sur nos vies et à agir de manière autonome, alors même que le paradigme agentique entre en contradiction directe avec les exigences de cybersécurité et de protection de la vie privée. Le terme même d'agent, qui n'a rien d'anodin sur le plan technique, désigne en réalité un système qui remplit deux fonctions. D'une part, pour pouvoir agir en votre nom, l'IA doit accéder à votre univers, à votre environnement, à votre contexte, autrement dit à vos données, de sorte qu'une masse considérable d'informations devient soudainement accessible. Ces données sont, très vraisemblablement, transmises ailleurs, car la puissance de calcul disponible sur la machine de l'utilisateur ne suffit généralement pas à les traiter localement. D'autre part, l'agent exploite ces données pour agir sans solliciter votre autorisation, puisqu'il doit précisément disposer d'une capacité d'action autonome. S'il devait demander une validation à chaque étape, il ne s'agirait plus d'un agent. Ce paradigme est donc déjà porteur de tensions, et nous constatons des pressions croissantes en faveur de l'intégration de ces agents, soutenues par des investissements massifs en capitaux et par la recherche du modèle adéquat pour le marché grand public.

À mes yeux, la rhétorique déployée autour de ces agents est irresponsable, au même titre que la manière dont ces organisations procèdent à leur déploiement. Le discours promotionnel insiste sur la simplicité d'usage, sur la promesse d'un génie magique qui accomplirait pour vous toutes les tâches administratives pendant que vous vous détendez mais les conséquences propres à ces systèmes agentiques, comme la réalité des conditions nécessaires pour leur permettre d'agir, sont passées sous silence. Pourtant, des violations de données existent déjà et nous voyons, par exemple, des utilisateurs laisser leur application Signal ouverte sur le web en raison d'erreurs de déploiement.

Chez Signal, cette évolution suscite une inquiétude majeure. Nous intervenons au niveau de la couche applicative et, comme beaucoup d'autres acteurs, nous devons pouvoir faire confiance au système d'exploitation. Or pendant des décennies, celui-ci a constitué une boîte à outils neutre. Aujourd'hui, nous assistons à ce que nous qualifions de « *coup d'État avec un gant de velours* » : une prise de contrôle de la couche applicative, dans laquelle l'accès aux données ainsi que la faculté d'en faire ce que l'on veut sont abandonnés aux trois entreprises qui exploitent les trois systèmes d'exploitation dominants, à savoir Android, Windows et iOS/macOS.

Prenons un exemple très simple : vous souhaitez qu'un agent organise un dîner d'anniversaire et invite vos amis. Pour que l'intelligence artificielle soit en mesure d'accomplir cette tâche, elle devra disposer de votre numéro de carte bancaire pour effectuer la réservation, de la capacité de simuler des clics de souris afin d'effectuer des recherches sur internet, de l'accès à vos messages Signal ainsi qu'à votre liste de contacts, et de l'accès à votre agenda pour vérifier vos disponibilités. L'ensemble de ces données hautement sensibles se trouve alors transmis à des sites externes, non seulement à celui qui traite directement vos données, mais également aux plateformes de réservation de restaurants, à l'application de calendrier, et à d'autres encore. À ce stade, toute frontière disparaît. L'octroi de tels accès ne crée pas une vulnérabilité simplement hypothétique dans notre protocole de chiffrement, qui constitue depuis dix ans l'étalon-or en la matière, il ouvre un vecteur d'attaque direct, créé par l'agent lui-même, permettant d'accéder à vos messages Signal dans le seul but d'organiser cette fête d'anniversaire. C'est bien ce que nous observons à travers le déploiement risqué de ces agents, dont l'architecture ressemble beaucoup plus à celle d'un logiciel malveillant qu'à celle d'une application ordinaire. Tout cela se fait sous couvert de facilité d'usage et d'enthousiasme pour l'IA, sans que les risques collatéraux fassent l'objet d'une attention suffisante.

Au sein de Signal, nous appelons à la suspension de ces déploiements risqués, dès lors que chacun d'entre nous dépend de ces systèmes d'exploitation, qu'il s'agisse de nos militaires, de nos gouvernements ou de nos familles. Nous ne pouvons accepter qu'ils soient ainsi vidés de leur substance par des agents qui les rendent globalement vulnérables. Nous appelons également à une amélioration substantielle de la documentation car, à mesure que ces systèmes sont déployés, la clarté diminue quant à leur fonctionnement, aux données auxquelles ils accèdent et aux destinations vers lesquelles celles-ci sont envoyées. Un surcroît de transparence est indispensable et il est tout aussi nécessaire que les développeurs puissent décider de ne pas recourir à ces dispositifs. Les équipes de Signal ne doivent en aucun cas être contraintes d'intégrer un agent ayant accès aux messages Signal, car un tel recours doit relever d'un choix propre à chaque application. Les utilisateurs peuvent eux-mêmes opter pour ces dispositifs, mais il nous faut être en mesure d'en bloquer l'accès, et ce blocage doit intervenir par défaut.

L'exemple de Microsoft Recall, annoncé il y a un peu plus d'un an avec Windows 11, est à cet égard éclairant. Il était présenté comme un outil offrant une mémoire exhaustive de l'ensemble des activités réalisées sur l'ordinateur, au moyen de captures d'écran effectuées toutes les quelques secondes, soumises à une reconnaissance optique de caractères (OCR), puis stockées, dans leur version initiale, au sein d'une base de données non chiffrée sur le système de fichiers, donc accessible à des acteurs malveillants. Ces captures incluaient notamment les messages Signal, exposant également les correspondants qui les envoyaient à cette captation intrusive. Face à cette situation, Signal a dû recourir à un mécanisme de type gestion des droits numériques afin d'empêcher une telle captation. Nous n'aurions pas nécessairement identifié ce besoin sans la vigilance d'experts particulièrement sensibilisés à ces enjeux, d'autant qu'aucune communication officielle n'avait été faite par Microsoft. Aucun choix ne nous a été laissé et nous avons dû agir pour protéger les utilisateurs de Signal sur Windows. Toutefois,

cette protection a reposé sur le seul levier disponible, avec pour conséquence de perturber des fonctionnalités d'accessibilité, notamment pour les personnes malvoyantes. Tel est l'état actuel de l'environnement, et il s'agit d'une question qui appelle une réponse urgente. Une attention beaucoup plus soutenue doit y être portée, en particulier par celles et ceux qui sont conscients de l'importance de l'intégrité et de la robustesse de nos infrastructures.

M. Éric Bothorel (EPR). Signal se présente comme un service éthique et centré sur l'utilisateur mais, à l'instar de toute grande plateforme, elle s'appuie sur des infrastructures critiques, souvent financées et régulées par les États, en particulier les infrastructures de télécommunication. Quelle est, dans ce contexte, votre position sur la notion de *fair share* ? Considérez-vous que Signal devrait contribuer davantage aux investissements consentis par les fournisseurs d'accès à internet dans les pays où elle opère, afin de garantir que la protection des données et l'accès aux services ne s'exercent pas au détriment de la souveraineté ou de l'intérêt public ?

J'aurais également une question d'actualité. Il semble que certaines organisations russes portent un intérêt particulier à Signal ou à WhatsApp. Elles n'exploiteraient pas des failles techniques, mais mèneraient des opérations d'hameçonnage. Plusieurs autorités européennes font d'ailleurs état, en la matière, d'une campagne d'une certaine ampleur visant des messageries, notamment la vôtre. Qu'envisagez-vous, le cas échéant, en termes de coopération, de prévention, ou au contraire d'absence d'intervention, afin de faire obstacle à cette opération ?

Mme Meredith Whittaker. Si je comprends bien la première question, vous demandez pourquoi Signal ne contribue pas plus aux infrastructures, par exemple de télécommunication. Je ne comprends pas bien la question.

M. Éric Bothorel (EPR). Comme Netflix et d'autres, vous êtes considérés comme des acteurs *over-the-top*. Cela signifie que vous vous appuyez sur des infrastructures déployées par des opérateurs qui investissent lourdement dans des technologies de câbles, de fibre ou de satellite. Il est question que les acteurs qui bénéficient de ces infrastructures pour le déploiement de leurs outils participent d'une manière ou d'une autre au financement de ces investissements. Est-ce plus clair ?

Mme Meredith Whittaker. Je pense qu'il y a, de votre part, une confusion entre Signal et des acteurs tels que Google ou d'autres entreprises de cette nature. Vous pouvez d'ailleurs constater les millions de dollars que nous consacrons à la bande passante, et je réponds ici à votre question car ces dépenses, particulièrement élevées, correspondent à des sommes versées aux acteurs qui nous permettent de fournir ces services. Nous opérons en tant que service *over-the-top* mais il ne nous est pas possible de procéder autrement. Voilà la réponse que je souhaitais apporter à votre première question.

S'agissant de votre seconde interrogation relative aux campagnes d'hameçonnage, il s'agit effectivement d'un sujet de préoccupation majeure. J'en discutais précisément aujourd'hui avec l'un de mes collaborateurs afin d'examiner les évolutions à apporter en matière d'interface, notamment pour garantir la mise en place d'alertes à destination des utilisateurs. Nous savons que la Russie, ainsi que d'autres États hostiles à Signal (vous savez que l'Ukraine recourt largement à notre application) sont des régimes autoritaires qui ne voient pas d'un bon œil l'accès des individus à leurs droits fondamentaux.

Mme Cyrielle Chatelain, rapporteure. Ma première question porte sur l'intelligence artificielle générative qui, au-delà des vulnérabilités en matière de sécurité, soulève des enjeux économiques, dans la mesure où elle capte aujourd'hui des volumes d'investissements considérables. Considérez-vous qu'il existe une forme de bulle autour de l'IA générative, susceptible de détourner des financements au détriment d'autres types de modèles qui pourraient pourtant présenter un intérêt ?

Ma seconde question concerne la captation des données. Vous avez indiqué que, pour permettre à un agent d'organiser un dîner, celui-ci devait accéder à un volume très important d'informations. Or des acteurs tels que Google disposent déjà d'un accès à nos courriels, potentiellement aux photographies que nous stockons, à nos carnets d'adresses ou encore à nos agendas, constituant ainsi des ensembles de données d'une densité exceptionnelle. Selon vous, ces données peuvent-elles être mobilisées à l'encontre des usagers ? Il me semble que vous avez évoqué, dans l'une de vos interventions, l'idée selon laquelle l'asymétrie d'information pouvait constituer un instrument susceptible d'être utilisé par des entreprises au profit d'États. Quel danger représente, dès lors, une telle concentration d'informations ?

Mme Meredith Whittaker. Sur la première question, je ne suis ni experte en finance ni vendeuse d'IA ce qui, dans cet univers, me confère une forme de singularité. J'observe les circuits du financement, le fonctionnement de l'économie, et il me semble en effet qu'il existe une forme de bulle. Je ne saurais toutefois en déterminer avec précision le point de cristallisation, compte tenu du niveau de richesse privée, du nombre d'entreprises cotées bénéficiant de financements considérables et du fait que les États-Unis paraissent avoir intérêt à la pérennisation de cette industrie en tant qu'instrument de domination. Le récit porté par ce secteur consiste à présenter l'IA comme l'aboutissement même du progrès, et il ne s'agit donc pas seulement d'un paradigme économique, mais également d'un paradigme géopolitique. Je ne dispose pas, pour ma part, d'un modèle prédictif permettant d'anticiper ce qui adviendra. Je peux certes envisager une certaine déflation et une atténuation de la courbe d'enthousiasme, mais quant aux effets à moyen et à long terme, je ne saurais les prédire. Je pourrais en revanche vous mettre en relation avec des personnes mieux armées que moi pour répondre de manière détaillée à cette question.

S'agissant à présent des dangers liés à la concentration des données, je ne crois pas qu'ils relèvent de l'hypothèse, et je ne crois pas non plus que nous puissions encore apporter des réponses rassurantes. Des exemples concrets permettent d'en prendre la mesure. Lorsque le régime hitlérien est arrivé au pouvoir, il a d'abord procédé à un recensement afin d'identifier les individus, leur origine et leur profession, et ce sont ensuite ces données qui ont servi au massacre de millions de personnes. S'il n'avait pas été possible de les identifier ni de les distinguer des autres sur la base de telles informations, un massacre d'une telle ampleur n'aurait pas pu se produire. Il nous faut donc reconnaître qu'il existe une asymétrie de pouvoir fondée sur l'asymétrie d'information.

Il faut également rappeler qu'aux États-Unis, une femme a été incarcérée après que Maga a pris connaissance d'un échange de messages sur Facebook entre elle et sa fille, dans l'État d'Alaska, à la suite de prises de position politiques de cet État en matière de reproduction. Elle avait aidé sa fille à accéder à des moyens de contraception, et elle est désormais en prison. Cet exemple nous est connu parce qu'il a été relayé par les médias, mais le problème excède très largement ce seul cas. Des entreprises détiennent des informations, alors même que des qualifications telles que « terroriste » ou « menace pour le pays » sont, par nature, mouvantes. Ce qui est légal aujourd'hui peut devenir illégal demain.

Ce que nous savons, en revanche, c’est que les entreprises qui nous surveillent détiennent des informations d’une extrême sensibilité. Au cours de mes treize années passées chez Google, j’ai pu observer la manière dont l’entreprise se reconfigure à l’occasion d’une élection présidentielle : tout y est alors réorganisé, depuis la stratégie de lobbying jusqu’aux personnes en poste, celles qui étaient proches de l’administration sortante étant écartées au profit de profils aussi proches que possible de la nouvelle équipe au pouvoir. À chaque alternance, ces entreprises cherchent à se placer au plus près du pouvoir afin d’en retirer des avantages, car leur finalité demeure la maximisation du profit. Les circonstances politiques évoluent mais les données, elles, demeurent. Ainsi, le compte Gmail que vous avez ouvert il y a plusieurs années pourrait fonctionner différemment sous un nouveau régime.

M. le président Philippe Latombe. Merci pour votre disponibilité, pour la franchise de vos propos et merci d’être venue discuter de ces sujets au sein de cette commission.

La séance s’achève à dix-huit heures quinze.

———

Membres présents ou excusés

Présents. – M. Éric Bothorel, Mme Cyrielle Chatelain, M. Philippe Latombe, Mme Laure Miller, M. Stéphane Rambaud, M. Alexandre Sabatou, M. Emeric Salmon, M. Hervé Saulignac

Excusé. – M. Philippe Gosselin