

A S S E M B L É E N A T I O N A L E

X V ^e L É G I S L A T U R E

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. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique..... 2

Jeudi

29 octobre 2020

Séance de 11 heures

Compte rendu n° 8

SESSION ORDINAIRE DE 2020-2021

**Présidence de
M. Philippe Latombe,
*Rapporteur***



**Audition, ouverte à la presse, de M. Bernard Benhamou,
secrétaire général de l'Institut de la souveraineté numérique.**

La séance est ouverte à 11 heures 05.

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, rapporteur. Je suis très heureux de vous accueillir, monsieur Benhamou. Vous êtes secrétaire général de l'Institut pour la souveraineté numérique (ISN). Notre mission d'information va, pendant plusieurs mois, se pencher sur moyens de bâtir et de promouvoir une souveraineté numérique européenne et française. Aussi nous apparaît-il indispensable de recueillir l'analyse de l'Institut que vous représentez parce que son objet de travail est identique à celui de notre mission.

À cet effet, nous souhaiterions que vous nous présentiez en quelques mots votre organisation, sa genèse, son mode de fonctionnement ainsi que ses activités.

Le thème de la souveraineté fait immédiatement appel au cœur régalien des missions de l'État, mais nous engage également à une réflexion sur les armes économiques dont nous devons disposer pour défendre la place de notre pays et de l'Union européenne dans la compétition mondiale. Sur ces deux plans, régalien et économique, nous aimerions connaître votre opinion sur la montée en puissance de la notion de souveraineté numérique. Comment l'analysez-vous ? Que pensez-vous des positions adoptées au niveau national et européen sur ces sujets par les autorités publiques ? Quelle appréciation portez-vous sur les initiatives législatives en cours ?

Cette problématique de souveraineté numérique implique de nombreux sujets souvent porteurs d'enjeux majeurs pour la place de notre pays sur la scène internationale. Nous pensons en premier lieu aux questions de cybersécurité et de cyberdéfense. Ici, la thématique de la souveraineté est incontournable puisqu'il s'agit de déterminer comment protéger les intérêts français de nouvelles menaces immatérielles et déterritorialisées. Il s'agit également de définir de nouvelles modalités de discussions avec nos partenaires européens et autres pour engager des actions concertées, mais respectueuses de la souveraineté de chacun. Quelle est votre analyse de ces enjeux multilatéraux ? Comment percevez-vous le paysage international actuel ? Quelles devraient être, selon vous, les réponses françaises et européennes aux menaces de déstabilisation ou de désinformation ?

La souveraineté numérique française et européenne est aussi, sur un mode peut-être moins visiblement conflictuel, confrontée à la montée en puissance de nouveaux acteurs privés qui prétendent imposer leurs normes ou qui disposent d'un pouvoir de marché les rendant bien souvent incontournables pour les consommateurs et les usagers. Comment la France et l'Union européenne peuvent-elles, selon vous, reprendre la main sur la définition des termes dans ces rapports nouveaux afin de ne pas être réduites à une position strictement réactive, voire passive ? Nous pourrions ici évoquer les multiples instances privées ou semi-privées dans lesquelles s'organise la gouvernance d'internet, l'attribution des noms de domaine par exemple, tout comme les géants du numérique qui jouent un rôle de prescripteur de plus en plus important dans nos sociétés, qu'il s'agisse des modes de consommation ou de notre façon de nous informer. La crise que nous traversons ne fait que renforcer malheureusement ces tendances. Quelle réponse publique apporter, selon vous, au plan national, européen et international ?

Enfin, la défense de la souveraineté numérique passe aussi par celle d'une certaine autonomie matérielle et par la défense et la promotion d'une industrie du numérique européenne compétitive et indépendante. Or nous savons que l'Europe souffre de façon croissante du départ d'industries stratégiques pour le matériel informatique qui constituent pourtant le soubassement du développement du numérique. La dépendance aux solutions technologiques extracommunautaires (aussi bien logiciels que matériels) met-elle en cause, selon vous, l'autonomie européenne ? Comment contrer cette tendance et comment faire participer l'innovation et la recherche à une certaine forme de réindustrialisation dans les nouvelles technologies à même d'assurer une plus grande souveraineté européenne ?

Je vous laisse la parole en espérant que nous pourrions balayer l'ensemble de ces sujets pendant l'heure qui nous est impartie. En tout cas, je vous remercie de vos commencements de réponse.

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. D'abord, l'ISN a maintenant six ans. Nous l'avons conçu en 2014-2015. À l'époque, la première question que l'on nous posait était : « Qu'est-ce que la souveraineté numérique ? » Je suis heureux de voir qu'après quelques années, on ne nous la pose plus. Aujourd'hui, le thème de la souveraineté numérique est devenu plus familier, parce qu'il est abordé quasiment quotidiennement dans la presse, mais tel n'était pas le cas à l'époque, quand nous avons créé l'Institut.

L'ISN est une association loi de 1901, qui rassemble des personnes de tous horizons (universitaires, entrepreneurs) et qui a été fondée sur l'idée que la question de la souveraineté numérique, qui apparaissait à peine dans le champ des experts et des régulateurs à l'époque, allait devenir importante.

À l'évidence, nous ne nous sommes pas trompés. Aujourd'hui, particulièrement du fait de la pandémie, l'on a pu se rendre compte encore plus de notre dépendance technologique à des solutions et à des acteurs extra-européens. En cette reprise de confinement, l'on se rend compte de l'importance, voire du déséquilibre que cela crée par rapport à notre tissu économique traditionnel. Fondamentalement aujourd'hui, l'on se rend compte de la véracité d'un propos que l'on avait tenu il y a quelques années qui consistait à dire qu'à mesure que les États utilisent les technologies, la souveraineté numérique devient indiscernable des outils technologiques. Quand il est question de défense, de sécurité, de sécurité sanitaire, de régulation des villes, d'éducation, de pratiquement tous les sujets sur lesquels la puissance publique a à se prononcer, aujourd'hui, le numérique a une part déterminante.

Je précise que j'ai aidé à créer l'ISN après avoir exercé les fonctions de délégué interministériel aux usages du numérique et, auparavant, de m'être beaucoup occupé au sein de l'État et de différents ministères des questions de régulation de l'internet, en particulier lors du sommet des Nations unies sur la régulation de l'internet en tant que conseiller de la délégation française. Ce sont des sujets qui maintenant sont montés en puissance. Vous parliez des grands acteurs non européens, qu'ils soient américains (Google, Apple, Amazon, Microsoft) ou chinois (Baidu, Alibaba, Tencent, Huawei, Xiaomi). Il manque dans ces acronymes des lettres européennes. S'il est bien une feuille de route pour la France et pour l'Europe dans les temps qui viennent, c'est bien de rajouter des lettres européennes dans ces acronymes.

Or, nous n'avons pas de grands acteurs de taille internationale dans ces domaines, ce qui est un prérequis indispensable si l'on ne veut pas agir que juridiquement. Quelle que soit l'efficacité des actions antitrust, quelle que soit l'efficacité des actions fiscales, quelle que soit l'efficacité des mesures de régulation que l'on peut être amené à prendre, si l'on n'a pas une industrie européenne forte dans ces domaines, ce qu'a rappelé Charles Michel, le président du Conseil européen, et Thierry Breton, le commissaire européen au marché

intérieur, si l'on n'a pas une industrie capable de concurrencer, voire de créer de nouvelles normes, de nouveaux standards dans ces domaines, comme l'a dit Sigmar Gabriel, l'ancien vice-chancelier allemand, tous les débats que nous évoquons aujourd'hui seront sans objet. Pour être un peu spécialiste de ces questions, pour l'enseigner à Panthéon-Sorbonne ou à Sciences Po auparavant, la régulation ne peut pas tenir si nous n'avons pas les acteurs.

Vous parliez de régulation à la fois sur les questions régaliennes et sur les questions économiques. La particularité réside dans le fait qu'il n'est pas de champ de l'activité économique de l'activité des États, des activités humaines de manière générale qui ne puisse de près ou de loin être transformée (« ubérisée ») par les acteurs numériques.

Auparavant, il existait des secteurs industriels qui étaient relativement stables (l'automobile, l'agriculture, le luxe, les transports...). Aujourd'hui, des acteurs qui n'ont aucune expérience préalable, aucune infrastructure préalable sont capables de s'insérer, de modifier, de transformer l'ensemble des modèles économiques. Ainsi, le groupe Accor, le célèbre groupe hôtelier français, n'imaginait pas il y a dix ans être confronté à un concurrent mondial, Airbnb, qui n'a possédé pendant très longtemps en propre aucune chambre d'hôtel, mais qui a été à même de vendre des nuitées partout sur la planète en l'espace de quelques années.

Pour l'instant, nous sommes en situation hautement défensive. Je crois qu'il nous faut absolument réfléchir à une possibilité de rebond, à une nécessité de rebond par rapport à cela. Cette nécessité doit prendre appui sur les faiblesses que nous notons aujourd'hui dans les acteurs du numérique, faiblesses en termes de confiance, faiblesses en termes de sécurité et de protection des données, faiblesses en termes de protection des processus démocratiques. Hier, les principaux patrons des réseaux sociaux étaient auditionnés au Sénat américain. L'on doit se poser la question de savoir dans quelle mesure on n'a pas laissé se produire des phénomènes tant en Europe qu'au niveau international de remise en cause des processus démocratiques. La triste actualité de ce matin nous rappelle les effets néfastes de la radicalisation algorithmique.

Ces plateformes, en plus d'exercer une influence de marché considérable, d'abuser très régulièrement de leur position dominante, de leur position monopolistique ou oligopolistique, ont un modèle économique basé sur la donnée personnelle. En termes techniques, on parle de « micro-profilage », c'est-à-dire de profilage extrême des individus. Ce modèle économique hyper-centré sur la donnée est toxique. Comme le disait une sociologue il y a quelque temps dans le *New York Times*, il n'existe pas de complicité entre le mouvement extrémiste djihadiste, suprématiste, *etc.* et les plateformes comme YouTube, mais il existe une convergence d'intérêts toxique.

Pourquoi ? Parce que l'algorithme de recommandations de YouTube intègre le fait que plus une vidéo est radicale (« hardcore »), plus elle est addictive et plus elle est addictive, plus les gens vont consommer de la publicité en la regardant. La radicalité, le côté clivant, polarisant, est utile à des plateformes comme Facebook ou comme YouTube et peut-être aussi sous une autre forme pour Twitter.

Nous avons laissé se construire ces sociétés en considérant que la donnée était l'or noir, le pétrole du siècle numérique, ce qui est très dangereux parce que cela tend à montrer que l'humain devient une matière première, une variable d'ajustement dans le fonctionnement de la société numérique. Je crois qu'il est important que la souveraineté numérique soit fondée, que l'action numérique européenne et française soit fondée sur les principes et les normes que nous défendons au sein de l'Union. Je citais les équivalents chinois des GAFAs américains, Baidu, Alibaba, Tencent, Xiaomi, qui se sont développés en voulant reproduire le modèle économique d'Amazon, de Google, de Facebook et d'Apple.

Nous devons avoir une vision innovante. Charles Michel, dans sa récente conférence de presse sur ces sujets, disait qu'il y avait un espace pour des technologies qui ne seraient pas menées soit par cette dérive liée à l'acquisition de plus en plus importante de données sur les individus, ce qui est le cas des grandes sociétés américaines, soit par cette vision autoritaire telle que la Chine la déploie chaque jour davantage autour du crédit social, c'est-à-dire ce système de notation orwellien des individus, une notation qui leur permet ou pas d'accéder à des droits fondamentaux comme celui de se déplacer en train ou en avion, d'accéder à un crédit ou à une promotion... Dans beaucoup de domaines, il s'agit d'un outil d'ingénierie sociale et de contrôle social extraordinaire efficace. Je précise que l'application de maîtrise de la covid en Chine qui a été élaborée par Alibaba est aussi un outil redoutable dans la mesure où l'on peut interdire de façon discrétionnaire l'accès à tel ou tel bâtiment, tel ou tel lieu public, tel ou tel service par l'intermédiaire d'un code que l'on doit scanner à l'entrée de chaque immeuble.

Quel modèle de civilisation voulons-nous ? C'est la seule bonne question qui vaille. Voulons-nous d'une civilisation qui serait régie par un contrôle permanent sur les individus ? Voulons-nous, pire encore, d'une civilisation où l'on obligerait tous les individus à se soumettre à des tests génétiques ? Je précise que des dizaines de millions de personnes sont soumises maintenant à des prélèvements à des fins de cartographie génétique totale de la population chinoise. Après le crédit social, on pourrait parler quasiment du génome social en Chine.

Nous devons nous tenir à égale distance de deux films de science-fiction.

D'une part, *Minority Report*, c'est-à-dire une société basée sur la surveillance absolue, totale et prédictive du comportement des individus. Ce n'est plus totalement de la science-fiction. Les forces de police, aux États-Unis et dans d'autres pays du monde, utilisent déjà des analyses *big data* pour pré-positionner les forces de police dans des endroits repérés comme ayant une forte probabilité de voir se produire des crimes ou des délits.

De l'autre, *Gattaca*, c'est-à-dire une société basée sur l'eugénisme et sur la génétique comme outil non seulement de traçage, mais également de contrôle et d'organisation sociale. Là encore, ce n'est plus tout à fait de la science-fiction. Aux États-Unis, la loi HR1313 a été présentée devant la Chambre des représentants. Elle avait pour but d'obliger à faire passer des tests à tous les employés des entreprises américaines à des fins de prévention des maladies. Les données auraient été détenues par les employeurs et les personnes qui refuseraient de se soumettre à ces tests auraient été sanctionnées à hauteur de 4 000 à 5 000 dollars par an. Cette loi n'est pas passée du fait de l'opposition des démocrates et, ensuite, du changement de majorité de la Chambre des représentants, mais elle illustre parfaitement cette tentation d'organisation sociale extrême, de rationalisation sociale extrême, de « solutionnisme technologique », pour reprendre l'expression d'Evgeny Morozov, de fascination pour l'efficacité technologique poussée à son extrême.

Puisque nous sommes en temps de pandémie, je rappellerai que des cabinets d'études sérieux avaient dit que le seul moyen de gérer à l'échelle mondiale une pandémie serait d'installer des capteurs de détection virale ou de menace biologique partout sur la planète pour en faire un réseau mondial qui détecterait les premières menaces où qu'elles apparaissent. L'auteur du rapport en question estimait que ce projet serait utile même si beaucoup de responsables politiques n'oseraient jamais le mettre en œuvre parce qu'ils ne mettront pas l'intérêt de leurs citoyens devant leurs considérations politiques.

L'on sait que ce projet se heurterait à des objections sur le caractère liberticide de ce genre de surveillance totale et instantanée, mais ce serait quand même le plus grand marché jamais entrepris en matière de technologie. Il existe cette fascination pour des solutions

liberticides, c'est-à-dire qui considèrent que démocratie, droits de l'homme, liberté sont des variables d'ajustement.

J'ai plaisir à le rappeler ici même, au sein de l'Assemblée nationale, en période de pandémie, parce que malheureusement, cette tentation a souvent été exprimée dans la période récente, c'est-à-dire de considérer que les libertés peuvent être mises entre parenthèses. Cicéron disait : « En temps de guerre, la loi se tait ». En temps de guerre pandémique, la loi devrait se taire. Non ! Si nous avons une possibilité de développer une activité autonome, indépendante des grandes plateformes asiatiques et américaines, c'est en nous appuyant sur les erreurs récentes, les fautes récentes qu'elles ont commises. Je pense à deux événements en particulier.

Le premier est l'affaire Snowden, la révélation des liens existants entre les services de renseignements américains et en particulier la NSA (*National Security Agency*) avec ces grandes sociétés. L'on a vu qu'elle a été à l'origine de la remise en cause du transfert des données des Européens aux États-Unis. La conséquence première de l'affaire Snowden pour nous, Européens, en plus d'apprendre le détail du fonctionnement et du niveau de surveillance que pouvaient établir des agences de renseignement dans ces domaines a été que la Cour de justice de l'Union européenne, en 2015, a eu l'occasion de remettre en cause le *Safe Harbor*, le premier accord transatlantique sur le transfert des données des citoyens européens aux États-Unis.

Cet accord, je le précise, était utilisé par plusieurs milliers de sociétés aussi bien aux États-Unis que dans d'autres pays. Auparavant, l'on considérait que les données transmises aux États-Unis étaient protégées, étaient relativement sûres et l'on s'est rendu compte que ces données pouvaient non seulement être analysées, mais être transmises pour essayer d'aider telle ou telle société. L'on pourrait citer le conflit entre Boeing et Airbus, mais les exemples ont été nombreux. Une crise de confiance à l'échelle mondiale, une crise de confiance systémique était sur le point de se produire par rapport à l'utilisation massive de ces données par des plateformes.

L'Union européenne, mal lui en a pris, a renégocié en urgence un autre accord, le *Privacy Shield*, qui vient, le 20 juillet dernier, d'être remis en cause par la même Cour de justice de l'Union européenne pour les mêmes raisons. Au départ, c'était juste après le scandale de l'affaire Snowden. Par la suite, cela a été le scandale de l'affaire Cambridge Analytica, l'utilisation des données des réseaux sociaux (Facebook en l'occurrence) à des fins de manipulation politique. L'on s'est rendu compte que les données des Européens ne sont pas protégées quand elles sont transmises de cette manière, compte tenu, en plus, du fait que les lois américaines s'appliquent de manière extraterritoriale, c'est-à-dire en dehors du territoire américain à des sociétés américaines basées en Europe.

Je rappellerai, pour ceux qui l'auraient oublié, qu'en janvier 2017, c'est-à-dire quelques jours après avoir pris ses fonctions de président des États-Unis, un certain Donald Trump émettait une ordonnance (*executive order*) privant les citoyens non américains de toute forme de protection de la vie privée dans le cadre des lois américaines. C'est ce qui avait valu à l'époque une interpellation de la part du groupe article 29, c'est-à-dire les commissions nationales de l'informatique et des libertés (CNIL) européennes, qui s'étaient interrogées sur la pertinence du *Privacy Shield*. Je précise que les responsables de la CNIL en France n'ont jamais reçu de réponse des autorités américaines.

À l'évidence, nous avons péché par naïveté, pour reprendre le terme employé par Thierry Breton dans sa tribune récente. Je rappellerai un propos que nous objectaient souvent nos interlocuteurs du département d'État quand nous étions aux Nations unies : « Vous, les Européens, vous ne savez que geindre. Vous n'avez pas d'industrie et la seule manière que

vous trouvez de nous ralentir, ce sont les actions juridiques. » Il faut bien comprendre que ces propos n'ont pas été seulement prononcés par Donald Trump dans la période récente, mais également par Barack Obama en 2015 qui déclarait, devant un auditoire d'entrepreneurs américains : « Les préoccupations élevées des Européens en matière de protection des données personnelles n'ont pour but que de nous ralentir parce qu'ils n'ont pas d'industrie, parce qu'ils n'ont pas créé l'internet. »

Cela est faux, je le précise, l'internet a été créé sur la base de travaux qui ont été menés en France par un certain Louis Pouzin qui a été récompensé par la reine d'Angleterre pour sa contribution à la création de l'internet au travers de technologies qui ont été élaborées en France. Le web a été lui aussi inventé en Europe par un Européen, Sir Tim Berners-Lee. De la même manière, l'une des innovations majeures des technologies de l'internet, qui équipe plus de 90 % des serveurs dans le monde, Linux, a été inventée en Europe par un Européen.

Nous, Européens, avons laissé les fruits commerciaux, stratégiques de ces révolutions se faire réappropriés par des sociétés qui ont su en tirer des bénéfices. « Il est temps d'en finir avec la naïveté », disait Thierry Breton. Cela est vrai du point de vue de la régulation où, enfin, l'on parle de mesures antitrust de manière claire, l'on parle de démantèlement, on parle de bloquer les marchés, on parle d'empêcher des fusions. L'Europe a accepté le rachat de WhatsApp et d'Instagram par Facebook alors qu'elle aurait dû s'y opposer.

Je précise qu'au début des années 2000, l'Union européenne était capable d'empêcher des fusions, y compris entre sociétés américaines. General Electric et Honeywell par exemple n'ont pas pu fusionner leurs activités sur les moteurs d'avions à cause d'une action européenne. L'absence de stratégie et de politique industrielle française et européenne, le fait que les grands projets européens aient essentiellement servi de variable d'ajustement pour de grands groupes et n'aient pas permis de développer un écosystème de petites entreprises innovantes et surtout de le faire croître. Tout le monde parle de la *Start-up Nation*. Je préférerais que nous soyons une *Unicorne Nation* ou, mieux encore, une *Big Tech Nation*. Excusez-moi de parler en anglais, mais en gros, je préférerais que nous ayons la capacité à faire grandir ces sociétés hormis par le rachat ou l'expatriation.

Or, pour l'instant, les quelques sociétés qui ont pu émerger dans ces domaines sont, la plupart du temps, obligées d'envisager un rachat par des structures étrangères. Il existe des mécanismes auxquels se sont opposés certains de nos partenaires européens comme l'Angleterre dans le passé sur le *Small Business Act*, les Anglais refusant de toucher aux marchés publics au nom de la distorsion de concurrence.

Non, les Américains pratiquent une politique industrielle extrêmement agressive, extraordinairement interventionniste là où nous sommes spectateurs, alors que nous devons devenir acteurs pour, comme le rappelait l'excellente économiste italo-américaine Mariana Mazzucato, que l'État assume son rôle de stratège, voire assume son rôle d'entrepreneur. Tel était le titre de son livre : *L'État d'entrepreneur*. Rappelons par exemple que les technologies fondamentales utilisées aujourd'hui dans l'iPhone, pour quasiment la totalité d'entre elles, ont été développées sur des crédits fédéraux américains. L'internet le premier a été développé sur fonds fédéral militaire, mais l'on pourrait parler des écrans tactiles, des interfaces vocales, des interfaces en réalité augmentée, pratiquement toutes les technologies clés ont pu être développées parce que la puissance publique a largement investi dans leur développement, parce que la puissance américaine, depuis plus de cinquante ans, a développé un mécanisme appelé le *Small Business Act*, c'est-à-dire une loi orientant une partie significative de la commande publique vers des PME innovantes.

Nous devons urgemment réfléchir à ces mécanismes. À chaque fois, l'on nous oppose : « Non, de toute manière, des financements, il y en a. » Mais ce qui importe, ce n'est pas que le financement, c'est pour des entreprises européennes d'être en mesure d'avoir la possibilité de faire évoluer leurs produits face à des clients solvables, et ce dans les premiers temps de leur création. Le *Small Business Act* et les possibilités d'orienter et d'aider la recherche sur des secteurs stratégiques, c'est ce qu'ont fait les Américains. Ils continuent de le faire dans le spatial avec SpaceX, qui repose de façon très importante sur les commandes publiques de la NASA, mais cela est vrai de pratiquement toutes les entreprises en termes de défiscalisation. Je lisais un article récent sur les usines que Tesla va créer en Europe et qui seraient, pour beaucoup, financées indirectement par des crédits européens. Je crois que, là encore, il nous faut rompre avec la résignation passive par rapport aux choix technologiques dans ces domaines.

Je parlais de sécurité sanitaire et de l'importance qu'elle pourrait avoir au niveau européen. Avec la pandémie, l'on voit bien que les données autour de la santé qui sont des données sensibles au sens de la CNIL deviennent extraordinairement stratégiques. Un projet, décidé un peu avant la pandémie, a été mis en place et accéléré pendant la pandémie : il s'agit du projet de plateforme des données de santé mis en place par le ministère de la santé. Ce projet réunit à lui tout seul tous les paramètres qui ont dysfonctionné dans les politiques industrielles en Europe et en particulier en France.

Je rappelle sa genèse. Ce projet est né à la suite du rapport de Cédric Villani sur l'intelligence artificielle qui préconisait que soient développés des outils d'intelligence artificielle en santé et, pour cela, de réunir les données de santé dans le cadre d'une plateforme, le *Health Data Hub*. J'en parle pour avoir travaillé dans les services du Premier ministre sur les questions d'administration électronique il y a fort longtemps. Quand on a un projet aussi stratégique, l'on doit s'interroger sur son impact sur l'écosystème technologique et sur ses missions à long terme. Or les deux n'ont pas été faits correctement.

D'une part, ce projet a été confié, pour son hébergement, à Microsoft, ce qui a suscité de nombreuses critiques et interrogations de professionnels de la santé. L'ancien président du comité d'éthique y a vu un cadeau insigne fait à la société Microsoft. Au-delà, l'on y a vu un risque sur l'évolution même du secteur de la santé.

Si vous me permettez une parenthèse dans la parenthèse, aujourd'hui, beaucoup de gens s'interrogent sur le devenir des GAFAM en disant : « Ils ont pu exercer leurs muscles sur des secteurs que l'on identifie assez bien, la publicité, les transports, *etc.* Les segments de croissance prioritaires pour ces sociétés aujourd'hui sont les services financiers et le secteur prudentiel, c'est-à-dire tous les services de banque et d'assurances. » Plus que de devenir des acteurs de la santé au sens traditionnel comme le sont les acteurs pharmaceutiques ou les acteurs du soin, ces sociétés qui ont acquis une somme considérable de données sur les individus sont capables de profiler les risques.

Qu'est-ce qu'un assureur ? C'est d'abord un acteur qui est capable de mesurer les risques pour chaque individu. Les grandes plateformes (Facebook, Google, Apple) sont en mesure de participer à l'analyse de données extraordinairement précises sur les individus et donc de proposer des assurances hyper individualisées, ce qui pour nous, Européens, et surtout pour nous, Français, semble très éloigné de notre modèle social de couverture mutualisée du risque. Vu d'un acteur technologique, il s'agit d'une opportunité considérable. Je recommande un extraordinaire rapport qui a été établi par la branche recherche de Goldman Sachs qui évoquait l'introduction des objets connectés dans le champ de la santé comme un vecteur possible d'économies de plusieurs centaines de milliards par an pour le système de santé américain. Ce rapport montrait que la prévention en matière de santé pouvait

devenir un outil d'économies considérables, et donc de bénéfices considérables pour les acteurs en question.

Je reviens sur la plateforme des données de santé. Nous ne devons pas nous préoccuper seulement des gains immédiats, mais nous devons avoir une vision stratégique sur ce que devient le secteur santé qui est, on le voit bien en période de crise pandémique, l'un des secteurs stratégiques pour l'ensemble des acteurs européens. Si l'on assistait à une « ubérisation » de l'assurance santé (je précise que Google a annoncé il y a quelques semaines sa première initiative d'assurance santé aux États-Unis et l'on ne doute pas qu'il ait l'intention de la déployer dans d'autres régions du monde), il faut se poser la question de l'évolution de ce secteur, de notre volonté ou pas d'empêcher que se mettent en place des solutions de contrôle, de monitoring des activités comme le font les objets connectés aujourd'hui, voire de maternage, pour inciter les individus à modifier leurs comportements.

L'on est capable de faire en sorte que ces technologies accompagnent les individus pour modifier leurs comportements. C'est déjà le cas d'un point de vue idéologique sur les réseaux sociaux : l'on se rend compte que l'on est capable de modifier et d'accentuer certaines réactions en fonction de l'état de l'humeur ou de l'histoire personnelle de chaque utilisateur. En matière de santé, il s'agit un peu de la même idée.

Comment devons-nous nous situer, nous Européens, dans l'évolution de ces technologies ? L'idée est de faire en sorte d'aider à développer des solutions éthiques, des solutions qui soient en accord avec les principes et valeurs des Européens. Maîtriser notre destinée numérique, c'est aussi maîtriser notre destinée politique dans ces domaines et essayer de faire en sorte de développer une voie alternative aux exemples de dérives sino-américaines. Récemment, lors d'un débat sur la 5G, un industriel déclarait : « Les Européens sont absents de ce débat ». Je lui répondais : « Non, les Européens sont présents dans ce débat : ils sont les proies. » Je précise que le ministre américain de la justice, M. William Barr, a eu l'occasion, dans le cadre de ce conflit avec la société Huawei, qui est l'un des grands acteurs de la 5G, de dire : « Nous devons, avec des sociétés alliées, prendre des participations majoritaires dans deux acteurs européens, Nokia et Ericsson, parce qu'ils possèdent un portefeuille de brevets important dans ces domaines. » D'alliés traditionnels, nous sommes devenus les proies que l'on vient dépecer pour renforcer la puissance industrielle américaine. Est-ce la destinée de l'Europe ? J'espère que non. Sommes-nous capables d'aider à développer des acteurs européens qui restent européens et qui ne sont pas soumis à des diktats sur le modèle économique comme le sont les diktats mis en place par Facebook, Google, Amazon ? Voilà la vraie question pour les temps qui viennent.

Je parlais de quelques mesures de régulation que sont le *Small Business Act*, l'aide à la commande publique, les actions de stratégie industrielle. Une autre action de coordination de la gouvernance des technologies a été prise aux États-Unis : la création, sous Barack Obama, d'un *chief technology officer* pour l'administration fédérale américaine. Il s'agit d'un coordinateur fédéral pour les technologies de l'État qui répond directement à la Maison-Blanche. Je crois qu'au niveau français et européen, nous aurions grand avantage à avoir ce type de fonction transversale qui analyse les technologies non pas seulement sur le plan industriel ou sur le plan des services rendus aux citoyens, mais bien sur le plan de leurs impacts sociétaux, culturels, sur l'ensemble de la population.

Je rappellerai que la ville de Toronto avait passé un accord avec Sidewalk Labs, une filiale de Google, pour gérer les technologies de la ville intelligente de Toronto. Plus les citoyens de Toronto ont été informés du détail des opérations qui se mettaient en place, plus ils se sont rendu compte que cela ressemblait au crédit social chinois, c'est-à-dire la notation systématisée, l'obligation de transparence par rapport aux données personnelles, les sanctions

pour les personnes qui n’obtempéreraient pas. S’est posée une question de souveraineté au sens premier. Les citoyens de Toronto ont dit : « Nous n’avons pas élu le patron de Google, il n’a pas à diriger nos vies. » Un mouvement d’opinion massif s’est mis en place et, en mai dernier, la filiale de Google en question a annoncé l’arrêt total de ce projet. L’on voit bien le risque du micro-profilage que j’évoquais tout à l’heure, c’est-à-dire l’acquisition d’une grande quantité d’informations sur les individus qui permet par la suite d’appuyer sur telle ou telle tendance pour les manipuler.

C’est ce que dit très bien l’excellente Shoshana Zuboff, professeure à Harvard, dans *L’âge du capitalisme de surveillance*, livre qui est traduit en français depuis quelques jours. Aujourd’hui, il n’est plus question simplement d’orienter le comportement commercial des individus. Le but est de modifier leur état d’humeur, de renforcer certaines convictions, de modifier leur comportement politique. Elle dit : « Nous croyons que nous cherchons avec le moteur de recherche Google, alors que c’est lui qui cherche en nous. » Toutes les informations que l’on donne à un moteur de recherche ne sont jamais perdues. Toutes les informations qui sont dans un réseau social sont rassemblées, traitées, échangées par des courtiers en données (« *data brokers* ») et constituent des profils d’une extraordinaire précision sur les individus. Devant le Congrès américain, Mark Zuckerberg a été obligé de reconnaître que Facebook récupérait, stockait et analysait des données sur des personnes qui n’étaient même pas des abonnés Facebook (« *shadow profiles* ») pour être en mesure d’étendre le niveau d’analyse et donc de recommandation publicitaire de Facebook, y compris de données médicales.

Je crois que nous devons nous poser des questions bien au-delà des simples questions industrielles, économiques traditionnelles. Ce dont relève aujourd’hui le numérique, c’est véritablement de questions politiques au sens profond, c’est-à-dire d’orientation générale de l’activité de notre société pour les temps à venir. C’est pour cela que nous devons aussi développer dans le même temps des régulations et une politique industrielle forte pour développer nos propres acteurs avec leurs propres orientations stratégiques.

M. Philippe Latombe, rapporteur. Merci pour ce propos introductif. Nous avons en Europe et en France en particulier des très bons industriels dans le domaine de la reconnaissance faciale. Nous avons certainement parmi les meilleurs dans ce domaine.

M. Bernard Benhamou, secrétaire général de l’Institut pour la souveraineté numérique. Je crains que les Chinois ne soient meilleurs.

M. Philippe Latombe, rapporteur. Les Chinois sont meilleurs parce qu’ils ont une partie de la « bibliothèque », ce que nous n’avons pas forcément. En France et en Europe, la reconnaissance faciale suscite un débat : faut-il l’autoriser ou l’interdire ? Nous sommes dans une espèce d’entre-deux où rien n’est autorisé et rien n’est interdit. Le fameux Livre blanc de l’Union ne l’a pas vraiment traité. Nous avons des questions qui se posent aujourd’hui, notamment en France. Vous avez parlé des valeurs et du « solutionnisme technologique ». La reconnaissance faciale est à la croisée de ces deux points. Qu’en pensez-vous ? L’Europe doit-elle interdire la reconnaissance faciale ?

M. Bernard Benhamou, secrétaire général de l’Institut pour la souveraineté numérique. Très peu de technologies sont intrinsèquement négatives. Je pourrais citer par exemple les technologies de *deepfake* qui permettent de déshabiller des individus de manière à les gêner voire à faire pression sur eux ou à les menacer.

Les algorithmes de reconnaissance faciale peuvent être sujets, comme ils l’ont été souvent aux États-Unis, à des discriminations et donc favorisent une reconnaissance efficace

des Caucasiens, c'est-à-dire des blancs, à la différence des Noirs ou des Afro-américains, où l'on a eu des cas d'arrestations à cause d'une reconnaissance faciale erronée.

Tout dépend de la manière dont ces technologies sont conçues. Je parlais tout à l'heure des systèmes bancaires. Apple, qui est devenue une banque en s'alliant avec Goldman Sachs, a mis en place des systèmes de crédit. Quelqu'un a remarqué qu'à revenu égal, une femme avait une espérance de crédit dix fois inférieure à un homme sur la plateforme d'Apple. L'on s'est rendu compte qu'il existait un biais, une discrimination algorithmique au sein de la plateforme. Cela a même été confirmé par le cofondateur d'Apple, Steve Wozniak.

Je crois que les technologies, y compris les technologies de reconnaissance faciale, mais aussi l'ensemble des technologies militaires (je rappelais les liens historiques entre la Silicon Valley et les financements militaires : beaucoup de projets initiaux de la Silicon Valley ont été à orientation militaire dans pratiquement tous les secteurs) peuvent être utilisées à bon ou à mauvais escient.

Comment ces technologies interviennent-elles dans le champ social ? Voilà ce qui me préoccupe. Va-t-on vers *Minority Report* avec une reconnaissance faciale généralisée, avec des risques de contrôle qui s'étendent au-delà du raisonnable ? C'est tout le débat. Que ces technologies puissent être utiles ou utilisables, bien sûr. Qu'elles doivent être généralisées au point que l'on rentre dans un système de surveillance totale comme c'est le cas en Chine, non. L'une des sociétés les plus valorisées dans le domaine de l'intelligence artificielle en Chine est justement une société sur la reconnaissance faciale, dont le principal client est le gouvernement chinois. Quelles limites donnons-nous à ces acteurs ? Quel modèle économique développe-t-on à partir de ces technologies ? Est-ce un modèle de surveillance absolue ? D'après le *Financial Times* qui a mené une enquête, certains *data brokers* réunissent déjà plusieurs centaines de millions de profils différents et plusieurs dizaines de milliers de paramètres par individu. Je pense qu'il est des modèles économiques qui sont toxiques. Avec l'affaire Cambridge Analytica, on a vu comment une frange de l'électorat était capable de basculer avec des campagnes de manipulation de masse hyper individualisée.

Il ne faut pas considérer qu'une technologie est mauvaise en elle-même sauf rares exceptions, mais considérer qu'une technologie doit être utilisée en ayant conscience de ce qu'elle peut générer. Quand on fait des tests génétiques massifs, on sait très bien que cela peut générer d'autres formes de surveillance encore plus inquiétantes. Quand on fait de la reconnaissance faciale à raison de plusieurs centaines de millions de caméras sur le territoire chinois par exemple, on sait très bien que cela correspond à une forme de dictature numérique, avec l'autosurveillance des individus et l'autocensure des individus, la surveillance par l'État, l'ensemble étant mis en œuvre avec des systèmes de reconnaissance faciale aussi. Là encore, c'est dans la manière dont ces technologies seront déployées que risquent de se trouver des problèmes ou des questions politiques et philosophiques sur le devenir de nos sociétés.

M. Philippe Latombe, rapporteur. Je vous pose une question que pose mon collègue Pierre-Alain Raphan. À votre avis, quelles actions doit-on mener à destination des citoyens pour les sensibiliser aux enjeux de cette économie de l'attention ? Que doit-on faire pour susciter une prise de conscience ? Nous avons quand même l'impression d'un manque d'information quant aux enjeux de cette économie de l'attention.

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. Vous avez parfaitement raison et vous remerciez votre collègue, le député Raphan, de cette question. Je crois qu'il est important de sensibiliser et d'éduquer. C'est l'ancien délégué aux usages de l'internet qui vous parle.

De manière générale, pour être efficace, il faut agir sur trois volets : l'éducation/sensibilisation, la régulation des technologies et la régulation juridique. Il ne faut pas faire reposer sur le citoyen l'essentiel du poids. Je crois qu'il est important d'informer le citoyen pour qu'il puisse constituer une force de réaction. Je vous parlais de la réaction citoyenne à Toronto, une réaction que je trouve remarquable. Il faut qu'il y ait une sensibilisation suffisante dans ces domaines.

Pour l'instant, nous en sommes au tout début. Il est évident que les plateformes dont nous parlons (Facebook, Google, *etc.*) ne perdront pas d'emblée des centaines de millions de leurs utilisateurs. Il faut arriver à réguler leurs comportements les plus toxiques et à faire en sorte que les acteurs de ce secteur, y compris les investisseurs, perçoivent les risques. Ils commencent à les percevoir.

Ainsi, la société Palantir qui fait le *big data* pour les services de renseignement américains a, malheureusement, été choisie à deux reprises par la DGSI (direction générale de la sécurité intérieure) pour gérer les données antiterroristes et a même proposé gratuitement ses services à l'AP-HP (Assistance publique-Hôpitaux de Paris) pour la gestion des données covid. L'AP-HP a refusé, mais nos voisins britanniques du NHS (*National Health Service*), eux, ont accepté. Cette société est rentrée en bourse il y a peu. Dans son dossier de présentation, elle indiquait : « Les modifications du paysage de la régulation pourraient être amenées à remettre en cause la nature même de notre modèle économique. » Ils ont raison !

Aux États-Unis, la majorité démocrate de la Chambre des représentants a émis un rapport très dur sur ces plateformes, et en particulier sur les aspects antitrust. Plus près de nous, la Chambre des communes britannique a qualifié dans un rapport ces plateformes de « gangsters numériques qui subvertissent la démocratie ». Je crois qu'il est temps de faire en sorte que l'écosystème, y compris les investisseurs, soit conscient qu'il existe un risque. Je pense qu'il s'agit d'un moyen de pression important, en plus des actions antitrust, en plus de l'ensemble des actions de régulation.

Je crois que la sensibilisation des citoyens est importante, mais ne sera pas suffisante. Elle doit être complétée par la régulation technologique et la régulation juridique. Le règlement européen sur les données est maintenant exporté dans de très nombreux pays, bien au-delà de l'Europe. Même les Chinois s'appuient sur le règlement général sur la protection des données (RGPD) pour développer leur propre législation sur la protection des données ! Nous devons aller vers une meilleure compréhension par les citoyens, par les responsables, par les régulateurs, par les législateurs. C'est l'ensemble de ce spectre d'actions qui doit être mené dans les temps à venir.

M. Philippe Latombe, rapporteur. Vous avez évoqué le *Small Business Act* et les capacités que les pouvoirs publics peuvent avoir non pas en accordant des subventions, mais en fournissant des contrats aux entreprises. Vous avez parlé du RGPD et de la réglementation. Vous avez évoqué les décisions de justice *Schrems I* et *Schrems II* très récemment. Je ne vous pose pas la question : y aura-t-il un *Privacy Shield 2* qui ferait un *Schrems III* ? Quelles seraient, dans les mois ou l'année qui vient, les mesures à prendre au niveau européen pour essayer de mettre ces barrières ? Si vous aviez une baguette magique et que vous étiez à la place de l'ensemble des décideurs, que proposeriez-vous ?

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. Si j'avais une baguette magique, j'empêcherais que l'on mette de côté les travaux de Louis Pouzin il y a cinquante ans pour aider à créer un internet européen.

M. Philippe Latombe, rapporteur. Si vous aviez une baguette magique qui fonctionne pour l'avenir et pas pour le passé, que feriez-vous ?

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. Je trouverais parfaitement regrettable que nous soyons soumis à un *Schrems III*, c'est-à-dire que l'Union européenne ne retienne rien des leçons du passé. Il est temps de mettre un terme à la naïveté, c'est-à-dire qu'il faudrait localiser les données en Europe (*data sovereignty, data localization* ou *data residency*). Les données des Européens doivent être traitées en Europe par des acteurs européens. Quand je dis des acteurs européens, pas des faux-nez, de vrais acteurs européens dont le siège et le quartier général sont en Europe. Certains disent, y compris dans l'exécutif, qu'une société comme Microsoft est une société européenne ! La définition est tangentielle parce que, malheureusement, le droit américain s'applique y compris pour les données stockées en Europe.

Nous avons donc besoin d'établir de nouveaux principes. Je précise que les acteurs américains avaient déjà anticipé ce durcissement des législations en créant des *data centers* en Europe. Il faut aller beaucoup plus loin. Je sais qu'une proposition de résolution européenne vient être proposée au Sénat par Mme Morin-Desailly sur ces questions, sur le fait d'obliger à traiter des données sensibles des Européens en Europe par des acteurs européens. Je pense qu'il faudra modifier nos textes. Il en va de notre sécurité nationale et de notre souveraineté. La sécurité nationale ne faisant pas partie des prérogatives sur lesquelles l'Union européenne a à se prononcer, il serait tout à fait possible de modifier les textes de manière à imposer que les sociétés traitant des données sensibles classiques (données de santé, politiques, ethniques, religieuses, philosophiques, sexuelles) et des données qui en apparence ne sont pas sensibles, mais qui le deviennent soient européennes. En analysant des données sur le comportement d'un individu, par exemple sur son périmètre de marche, l'on est capable de prévoir s'il va avoir des maladies ou pas. En analysant son comportement avec la montre connectée d'Apple, l'on peut prévoir les crises de panique.

Il faut bien comprendre qu'il y aura en même temps à déterminer une stratégie industrielle pour faire en sorte que les Européens développent leurs marchés et leurs technologies et évitent de transférer des données à l'étranger, sur lesquelles ils n'ont plus de contrôle. Je rappelle que les *data brokers* qui échangent entre eux des données, qui vendent parfois des profils à des administrations, sont une sorte de trou noir pour la régulation sur les données. Les acteurs qui ont développé le RGPD disent que cela ne tiendra pas.

Il faut aider à créer un cadre beaucoup plus protecteur pour les données et, en amont de la collecte, se poser la question de savoir si certaines données ne doivent pas faire l'objet d'une extraction, ne doivent pas être traitées. Il s'agit d'une vraie question pour les temps qui viennent. À partir de quand devra-t-on empêcher que certaines données puissent être traitées ? Des chercheurs viennent de publier dans *Le Monde* d'aujourd'hui une critique sur les questions de sécurité concernant le *Health Data Hub* en disant : en concentrant les données à un seul endroit, l'on crée un point de vulnérabilité important, un point d'attaque possible. De nombreuses questions s'entremêlent autour de cela, mais la principale des baguettes magiques, c'est qu'il y ait une prise de conscience parmi l'ensemble des citoyens, des acteurs et des régulateurs dans ces domaines. Nous n'en sommes qu'au tout début.

M. Philippe Latombe, rapporteur. Merci beaucoup.

La séance est levée à 12 heures 05.



Membres présents ou excusés

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

Réunion du jeudi 29 octobre 2020 à 11 heures

Présent. - M. Philippe Latombe

Excusées. - Mme Virginie Duby-Muller, Mme Frédérique Dumas, Mme Laure de La Raudière, Mme Nathalie Serre