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

– Audition, ouverte à la presse, de M. Martin Untersinger, journaliste au Monde, et MM. Antoine Schirer et Sébastien Bourdon, journalistes indépendants 2

– Présences en réunion 15

Jeudi
26 mars 2026
Séance de 10 heures

Compte rendu n° 12

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à dix heures.

M. le président Philippe Latombe. Monsieur Untersinger, vous avez mené une enquête pour le journal *Le Monde* sur les entreprises qui font le commerce des données personnelles sur internet. Messieurs Schirer et Bourdon, vous avez signé la semaine dernière un article, dans *Le Monde* également, alertant sur le fait que vous étiez parvenus à localiser précisément le porte-avions *Charles-de-Gaulle* en Méditerranée grâce à l'application Strava, utilisée par un militaire faisant son footing sur le pont.

Vos enquêtes montrent à quel point l'utilisation des données personnelles peut constituer un risque non seulement pour les individus mais aussi pour la souveraineté nationale.

Avant de vous céder la parole, je vous rappelle que l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission d'enquête de prêter serment de dire la vérité, toute la vérité, rien que la vérité.

(MM. Martin Untersinger, Antoine Schirer, et Sébastien Bourdon prêtent successivement serment.)

M. Martin Untersinger, journaliste au *Monde*. Je travaille depuis plus de quinze ans sur le numérique et les questions qu'il pose en matière de désinformation, de libertés publiques, de données personnelles, de grandes plateformes et de cybersécurité. Si vous espérez de ma part des solutions, vous serez déçus. En revanche, je peux partager mes constats.

Au risque d'enfoncer quelques portes ouvertes, je décèle trois types de vulnérabilité de l'économie européenne dans le domaine numérique.

Elle concerne d'abord les couches dites basses du cyberespace – la typologie en identifie trois –, c'est-à-dire les matériels, les équipements, les protocoles. Je laisse de côté ce sujet, qui ne me paraît pas premier et que je ne maîtrise pas pleinement.

Ensuite, la vulnérabilité affecte la couche des logiciels, soit tous ces outils que nous utilisons dans notre vie quotidienne, personnelle ou professionnelle et qui sont, pour leur quasi-totalité, conçus ailleurs – aux États-Unis, mais pas seulement. Je parle là des algorithmes des réseaux sociaux, des logiciels qui font fonctionner les téléphones et les ordinateurs, une large majorité des logiciels professionnels, les grandes plateformes utilisées par tout un chacun.

Est enfin vulnérable la troisième couche, qui permet de capter les usages, donc les données – personnelles mais pas seulement – que nous produisons et qui sont ensuite stockées, analysées et exploitées par des entreprises étrangères.

Les conséquences sont de trois ordres.

D'abord économique, l'innovation et les emplois se développant ailleurs et l'État étant dans l'impossibilité d'actionner ses leviers d'influence habituels sur l'économie.

Les conséquences sont ensuite d'ordre juridique avec, avant tout, la difficulté à appliquer notre droit puisque les entreprises sont implantées à l'étranger. Le code influe sur les usages – Lawrence Lessig a montré dès 2000 que « *code is law* » – et une part croissante de notre espace public et démocratique est régentée par des algorithmes conçus ailleurs. Par

exemple, lorsque le propriétaire du réseau social X décide de privilégier certains contenus, compte tenu du rôle de ce réseau dans la fabrique de l'information, cela a un effet concret, immédiat et dévastateur.

Enfin, toute l'architecture numérique est orientée vers la captation de notre attention et donc de nos données personnelles – les deux se nourrissant d'ailleurs mutuellement. À cette infrastructure s'arriment des dispositifs juridiques qui permettent aux autorités extra-européennes de récupérer ces données sous certaines conditions.

J'aimerais appeler votre attention sur plusieurs points.

D'abord, la souveraineté n'est pas la garantie de la sécurité : ce n'est pas parce que c'est fait en France ou en Europe que c'est automatiquement mieux. Parmi les très nombreux exemples, je mentionnerai le fait que les géants du numérique sont les seuls à offrir, pour les messageries, des moyens de protection à la mesure des menaces qui pèsent sur certaines populations à risque – journalistes, activistes, etc. Si je prends l'exemple du Health Data Hub, la plateforme des données de santé, lesdites données sont-elles réellement moins sécurisées sur cette plateforme qu'elles ne l'étaient auparavant dans des bases de données diverses et au régime de sécurité peut-être plus aléatoire ? Par ailleurs, il ne faut pas oublier les entreprises ou les services qui paraissent français mais qui sont en fait fondés sur des technologies ou des fonds américains.

Ensuite, il ne faut pas se laisser piéger par le discours lancinant selon lequel l'espace numérique serait sans règles et sans loi, et la puissance publique démunie et inopérante si elle ne s'appuie pas sur les géants du numérique. L'histoire récente montre que c'est tout bonnement faux. Le législateur, en particulier européen, est capable d'adopter des textes pour contraindre les géants du numérique – le RGPD (règlement général sur la protection des données), le DSA (règlement sur les services numériques), etc. Il suffit parfois d'appliquer les textes qui existent, ce qui ne va pas sans poser des problèmes d'application – nous parlerons sans doute des courtiers en données – ou de montrer que l'État dispose d'outils, tels que l'interpellation du fondateur d'une messagerie pour lui rappeler ses obligations.

Enfin, la gouvernance du monde numérique échappe en partie aux logiques strictement étatiques et économiques traditionnelles. Je pense notamment aux délibérations techniques, collectives et publiques dans des instances dédiées – par exemple sur les protocoles qui font fonctionner une grande partie de nos échanges numériques – ou aux modes d'élaboration de certains logiciels collaboratifs, transparents et accessibles à toutes et à tous, comme le logiciel libre. Ces initiatives ne sont pas strictement françaises, ni européennes, pourtant elles servent le bien commun.

M. Antoine Schirer, journaliste indépendant. Je suis journaliste indépendant. Je travaille pour des services d'enquête à la BBC, pour Reporters sans frontières et pour *Le Monde*.

Les StravaLeaks sont une série d'enquêtes qui examinent les vulnérabilités causées par un usage imprudent de l'application américaine Strava. Disponible sur les smartphones et les montres connectées, elle est l'application de sport la plus populaire – fin 2025, elle revendiquait, dans son rapport annuel, 180 millions d'utilisateurs actifs dans le monde. Elle permet aux utilisateurs d'enregistrer leurs performances sportives, mais aussi de les partager en ligne, un peu à la manière d'un réseau social. Le problème vient de ce que lorsque vous créez un profil sur cette application, celui-ci est, par défaut, public. On peut donc y trouver plein

d'informations, parmi lesquelles le nom, l'âge, mais surtout l'historique des activités, lesquelles sont souvent géolocalisées – on peut connaître le point de départ, le trajet et le point d'arrivée.

Notre enquête s'est intéressée à une autre fonctionnalité de l'application, qui permet de voir les autres personnes qui font ou ont fait le même trajet que vous. Si c'est dans le bois de Vincennes, cela ne pose guère de problème. En revanche, si des personnes dont le profil est public ont enregistré des activités dans des endroits plus sensibles, auxquels seuls certains individus ont accès – au hasard, les résidences du chef de l'État, des bases militaires –, elles apparaîtront sur l'application. C'est cette brèche que nous avons explorée.

Elle n'est pas nouvelle puisque, dès 2018, le *New York Times* avait réussi, par le biais de l'application, à localiser des bases américaines en Afghanistan. Dans la foulée en France, *Le Canard enchaîné* et *Le Télégramme* ont identifié des agents de la DGSE (direction générale de la sécurité extérieure) et des militaires sur la base de l'île Longue.

Dans notre premier travail, en 2020 pour *Mediapart*, Sébastien Bourdon et moi avions trouvé plus de 800 militaires français ayant participé à des opérations extérieures (Opex), dont plus de 200 membres des forces spéciales. En 2024, cette fois pour *Le Monde*, nous avons retrouvé des gardes du corps de trois chefs d'État – Joe Biden, Vladimir Poutine et Emmanuel Macron. S'agissant de ce dernier, les activités sportives des membres du GSPR (Groupe de sécurité de la présidence de la République) – les gardes du corps du président – nous ont permis d'identifier à l'avance et à dix reprises, les hôtels où séjournait le président lors de ses déplacements – ces informations sont censées être confidentielles – et de trouver les domiciles des agents, ce qui, selon une source proche du GSPR, constitue une faille de sécurité avérée.

Quelques mois plus tard, nous révélions comment des membres d'équipage des sous-marins nucléaires français divulguaient, par le biais de Strava, des informations sensibles sur le calendrier des patrouilles.

Enfin, la semaine dernière, avec nos collègues du *Monde* Asia Balluffier et Liselotte Mas, nous avons retrouvé la position du porte-avions *Charles-de-Gaulle*, rendue publique en temps réel par l'activité sur Strava d'un militaire.

Je peux d'ailleurs annoncer à votre commission que nous ferons prochainement de nouvelles révélations sur ce dossier ; nous sommes en bouclage.

M. Sébastien Bourdon, journaliste indépendant. Je suis également journaliste indépendant. J'ai travaillé pendant plusieurs années essentiellement pour le service enquête de *Mediapart* et plus récemment pour *Le Monde*, journal pour lequel j'ai cosigné avec Antoine Schirer les enquêtes sur Strava.

Mme Cyrielle Chatelain, rapporteure. Vos travaux ont ceci de différent que dans un cas, l'utilisation des données géolocalisées est volontaire – des personnes les affichent volontairement sur leur application – ; dans l'autre, elle donne lieu à une exploitation commerciale par le biais de courtiers en données. Dans tous les cas, cette utilisation pose des questions de sécurité, comme l'identification de personnalités aux responsabilités importantes, de proches ou d'habitudes. Pouvez-vous préciser comment ces données, qui paraissent inoffensives de prime abord, finissent, une fois compilées, par représenter un risque, en particulier dans la période de forte tension que nous connaissons ?

M. Martin Untersinger. En effet, nos enquêtes ne concernent pas tout à fait les mêmes données, mais les risques sont assez similaires.

J'ai travaillé avec des confrères de plusieurs médias européens sur des échantillons de données personnelles que nous nous sommes procurés auprès de courtiers en données (*data brokers*). Ces données, souvent géolocalisées, sont captées au sein d'applications de tous types, installées sur des téléphones, souvent à des fins publicitaires. Elles sont extraites, échangées et transférées sur un marché assez opaque et massif.

De la même manière que pour Strava, nous parvenons, à partir de ces données, à identifier des officiers de la DGSE, des policiers de la DGSI (direction générale de la sécurité intérieure), des militaires opérant sur des bases sensibles, des employés de grandes industries de défense, des personnels chargés de la protection de la présidence de la République, etc. Cela représente-t-il un risque ? Oui, celui-ci étant évidemment différent selon les personnes concernées.

Dans le cas des officiers de la DGSE, dont l'identité est protégée par la loi, savoir où ils habitent peut les exposer à des pressions. Ces données révèlent aussi leurs déplacements, leurs activités personnelles ainsi que leurs contacts. Elles représentent donc un risque évident. Cela vaut aussi pour les autres personnels que j'ai évoqués.

Les données sur lesquelles nous avons travaillé ne permettent pas de prévoir, contrairement à celles que mes collègues ont mentionnées, puisqu'elles concernent le passé. Mais elles donnent accès au même type d'informations – par exemple, la géolocalisation d'un gendarme de la Garde républicaine dans le petit village de la Creuse dans lequel Emmanuel Macron s'est rendu il y a quelque temps – ; on connaît précisément l'adresse de l'établissement hôtelier grâce aux données GPS.

Lorsqu'on se penche sur les déplacements des officiers de la DGSE, on les voit évidemment boulevard Mortier ; le long des lignes de métro qui les amènent à la gare du Nord ; sur les quais des trains de la gare du Nord qui desservent leurs lieux d'habitation ; devant chez eux, etc. C'est d'une grande finesse. Donc les risques sont nombreux. Les données sont en elles-mêmes inoffensives, mais dans la mesure où elles sont reliées au domicile, au lieu de travail et à tous les lieux qui permettent d'identifier la personne et ses activités habituelles, elles constituent une menace.

M. Sébastien Bourdon. Les risques sont *grosso modo* les mêmes pour les données sur lesquelles nous avons travaillé, à cette différence près que les données de Strava sont directement accessibles à tout un chacun – pas besoin d'un intermédiaire. Il suffit de créer un compte ; c'est gratuit et ne demande qu'une adresse e-mail et quelques clics.

Les personnes n'ont, pour beaucoup d'entre elles, pas conscience de ce qu'implique le fait d'appuyer sur un bouton sur une montre connectée ou sur un téléphone – ce faisant, elles mettent en ligne des données. Je le répète, le profil créé sur Strava est par défaut public, ce qu'ignore l'immense majorité de ses utilisateurs, comme ceux de Facebook ou d'autres réseaux sociaux. Ils ne vont pas davantage modifier les paramètres de l'application pour que leur profil devienne privé. Pourtant, les outils mis à disposition sont plutôt bien faits – deux clics et quinze secondes sont suffisants. Dès lors que le profil est privé, on limite une très grande partie des risques. On peut certes trouver des informations sur des profils privés mais l'immense majorité de celles que nous avons recueillies n'aurait pas pu l'être si les profils des gardes du corps ou des personnes sur le *Charles-de-Gaulle* avaient été privés.

J’y insiste, la plupart des personnes ne mesurent pas complètement ce qu’implique l’enregistrement de leurs performances sportives dans une application qui s’apparente à un réseau social. Les courses, les circuits de vélo qui sont enregistrés dans un profil sont automatiquement partagés ; ils peuvent être commentés, likés comme on le ferait sur Facebook avec ses amis.

Indépendamment de la différence de nature des données concernées, les risques sont exactement identiques à ceux que vient de mentionner mon confrère.

Dans notre cas, compte tenu des profils auxquels nous nous sommes intéressés – gardes du corps de chef d’État, sous-mariniers des SNLE (sous-marin nucléaire lanceur d’engins) ou marins à bord du *Charles-de-Gaulle* –, les risques opérationnels, notamment en matière de sécurité, sont évidents. Il est problématique que tout un chacun puisse, en trois clics, savoir où se trouve le porte-avions, ou connaître le rythme des patrouilles des SNLE ou la date de leur départ en mer – nous parlons là de l’une des composantes de la dissuasion nucléaire française.

Je prends un exemple très concret, qui date de 2024, si mes souvenirs sont bons. À Krasnodar, en Russie, un officier de l’armée russe a été assassiné pendant qu’il faisait un footing dans un parc, *a priori* par les services de renseignement militaire ukrainiens. Cet officier avait un profil Strava public et suivait toujours le même itinéraire. Il a vraisemblablement été attendu par ses assassins dans le parc où il avait ses habitudes. Certes, la situation en France n’est pas la même, mais le risque que représente le fait de pouvoir connaître les habitudes sportives d’agents ou de militaires est très clair.

À cela s’ajoute une dimension plus personnelle. Les gardes du corps qui côtoient toute la journée les présidents américain, russe ou français voient et entendent des choses sensibles. Un service de renseignement étranger disposera grâce à Strava d’un moyen de pression gigantesque sur la personne puisqu’il connaîtra l’adresse de son domicile, de l’école de sa fille, etc. Il pourra lui demander d’aller placer un micro à l’Élysée ou que sais-je encore.

Tout ceci est faisable très facilement. Mon collègue et moi avons certainement des compétences pour mener des enquêtes, mais avec des moyens très rudimentaires – un ordinateur et une connexion internet –, il ne nous a pas fallu plus de vingt-quatre heures pour repérer la position du *Charles-de-Gaulle* – nous ne travaillons pas à temps plein depuis deux ans sur le sujet. Il va donc sans dire que d’autres personnes, peut-être plus mal intentionnées, et dotées de moyens bien plus importants que nous, peuvent trouver ces mêmes informations, et même beaucoup plus.

M. le président Philippe Latombe. Pensez-vous que les applications devraient proposer par défaut un profil privé – une action serait ensuite nécessaire pour le rendre public – et non l’inverse ? Ce serait une mesure de sécurité minimale que le législateur pourrait imposer.

M. Sébastien Bourdon. Ce serait merveilleux, mais c’est totalement contraire au fonctionnement et à l’économie des réseaux sociaux, qui ont tout intérêt à ce que le maximum d’informations soient publiques. Cela me paraît assez inenvisageable.

Mme Cyrielle Chatelain, rapporteure. Avez-vous noté, à la suite de vos enquêtes, une prise de conscience au sein de l’armée, dont témoigneraient des directives enjoignant aux militaires de rendre privé leur profil ?

Pouvez-vous confirmer que Strava continue à stocker les données même si le profil est privé ?

Quel est le niveau de consentement à la captation de ces données ? Les utilisateurs en sont-ils conscients ? Le RGPD est-il respecté ?

M. Antoine Schirer, journaliste indépendant. Pour chaque enquête, nous avons eu des échanges avec l'armée. Nos interlocuteurs avaient conscience du problème et le prenaient très au sérieux.

On constate qu'après la parution de chaque article, des profils passent en privé, mais quelques mois plus tard, de nouveaux profils publics apparaissent. Il semble très compliqué de faire la police auprès de dizaines de milliers de militaires et de s'assurer que les règles d'hygiène numérique sont respectées.

M. Sébastien Bourdon, journaliste indépendant. La prise de conscience par l'armée des risques liés au numérique et aux réseaux sociaux est antérieure à nos articles. En 2020, lors de notre première enquête sur Strava, qui concernait les militaires en opération extérieure et les forces spéciales, nous avons appris que l'armée distribuait, depuis le début des années 2010, un guide – assez bien fait – du bon usage des réseaux sociaux, d'une dizaine de pages. Il y est indiqué comment mettre son profil en privé ; à quoi faire attention ; ce qui est autorisé et ce qui ne l'est pas. Ce document est régulièrement mis à jour et distribué à l'ensemble des militaires. La formation et l'information sont donc présentes au sein de l'armée. Nous savons que les recommandations, en particulier s'agissant de Strava, ont été renforcées à la suite de nos enquêtes. Pour autant, il faut conserver à l'esprit que le *Charles-de-Gaulle* accueille à son bord 1 800 marins. Comment vérifier concrètement que chacun d'eux applique les recommandations, pourtant salutaires dans un contexte de tension, et met son profil en privé ? Je n'ai pas la réponse.

M. Martin Untersinger. En ce qui concerne les données publicitaires, la légalité est une question centrale et finalement assez simple. Le droit européen est très clair : lorsque vous captez des données à caractère personnel pour faire de la publicité, en particulier lorsque cette captation se fait sur un appareil personnel, le consentement est obligatoire.

Comment ce consentement est-il obtenu dans le cas des données publicitaires que se procurent les courtiers en données personnelles ? Par la fameuse fenêtre que l'on appelle parfois de manière abusive la fenêtre RGPD – en l'occurrence, c'est la directive ePrivacy qui s'applique –, dans laquelle on vous informe que vos données personnelles sont captées par l'application et qu'elle les partage avec un certain nombre d'entreprises partenaires. Au début, il y en avait entre dix et quinze – ce qui est déjà beaucoup – mais, aujourd'hui, dans n'importe quelle application, vos données personnelles peuvent être transmises à plusieurs dizaines voire plusieurs centaines d'entreprises partenaires.

Si ces entreprises étaient effectivement les destinataires finaux et uniques des données, cela poserait déjà un certain nombre de problèmes, mais ce n'est même pas le cas. Mes collègues de la rédaction allemande du site *Netzpolitik*, avec lesquels j'ai travaillé, comparent le marché des données publicitaires mobiles à la lave à l'intérieur des lampes – elle bouge, se divise, se rapproche. Autrement dit, c'est un marché en mouvement permanent. Les données s'échangent, se revendent, sont modifiées, recoupées, etc. par des dizaines et des dizaines d'acteurs différents, sans qu'il soit vraiment possible de suivre leur cheminement.

En droit européen, le consentement doit obéir un certain nombre de règles : il doit être éclairé, libre, etc. Les conditions ne sont évidemment pas remplies pour les données que l'on retrouve chez les *data brokers* ou dans une régie publicitaire. Le marché repose sur une illégalité manifeste. Dès lors, la solution n'est pas – je suis désolé de le dire dans cette enceinte – d'adopter de nouveaux textes mais d'appliquer ceux qui existent et de donner aux régulateurs les moyens de s'attaquer à ce marché, qui est très clairement hors de contrôle.

M. le président Philippe Latombe. Puisque vous évoquez le RGPD et la directive ePrivacy, avez-vous un avis sur la future directive omnibus ? Va-t-elle améliorer ou dégrader la situation ? Va-t-elle accroître la masse de données dans les mains des courtiers ?

Le règlement omnibus touche à la définition de ce qu'est une donnée personnelle et tend à intégrer la directive ePrivacy dans le RGPD.

M. Martin Untersinger. Je ne suis pas au fait des dernières évolutions de l'omnibus. Il a effectivement été question de changer la définition des données personnelles. À cet égard, il est intéressant de noter que cet élément était réclamé par tous les géants du numérique ; toutes leurs contributions publiques le mentionnaient. Je vous laisse en tirer les conclusions sur l'impact que cela pourrait avoir sur nos libertés publiques. Mais je m'arrêterai là, car je ne suis pas familier des détails de l'omnibus.

Mme Cyrielle Chatelain, rapporteure. Vous dites qu'il conviendrait de donner davantage de moyens aux régulateurs, mais quelles sont les instances pertinentes ? S'agit-il de la Cnil (Commission nationale de l'informatique et des libertés), des instances de contrôle des données au niveau européen, de toutes à la fois ? Quels organes mériteraient de voir leurs capacités d'action renforcées ?

M. Martin Untersinger. Dans la mesure où le respect du droit relatif aux données à caractère personnel relève en France de la Cnil et, en Europe, de ses homologues, ces instances semblent être les chefs de file naturels pour régler ce problème.

Le premier enjeu est le caractère mouvant de cet écosystème très opaque, dans lequel il est très complexe de reconstituer le circuit des données. Pour avoir échangé avec la Cnil, je sais que les enquêtes et les procédures de sanction prennent du temps et que les entreprises concernées sont extrêmement agiles et fluides.

Ce n'est pas directement lié à une action du régulateur, mais j'ai en tête le cas d'une start-up française qui avait été épinglée par Google pour ne pas avoir respecté les bonnes pratiques sur son réseau publicitaire. Cette start-up récupérait des données personnelles pour les revendre, notamment dans des outils de surveillance proposés à des États. Une fois blacklistée par Google, cette société a disparu. Son PDG en a immédiatement recréé une autre et si je n'ai pas d'informations à son sujet, il n'y a, à mon sens, guère de suspense quant à son activité.

Il y a donc une complexité inhérente du marché, ainsi qu'une complexité technique. Pour avoir échangé avec des chercheurs informatiques, qui dédient une grande partie de leur activité à la compréhension fine des places de marché automatisées, des procédures de captation des données sur les téléphones et donc de toute la chaîne de transmission jusqu'aux courtiers, je peux vous dire qu'eux-mêmes, alors qu'on pourrait imaginer qu'ils disposent de moyens pour éclaircir le circuit des données, peinent à comprendre le cheminement. Ils font face à des acteurs qui opèrent à dessein dans l'opacité, précisément parce que cela leur permet de détourner un certain nombre de données au sein des marchés publicitaires. De plus, les entreprises qui

collectent les données sur les appareils sont ingénieuses pour déjouer les protections techniques qui s'y trouvent. Il y a un double enjeu de complexité organisationnelle et de complexité technique du marché.

Le problème des données personnelles est gigantesque. Les autorités de protection font avec les moyens qui leur sont conférés, sachant que les données publicitaires mobiles ne sont que l'une des questions qu'elles ont à traiter. Cela étant, à mon sens, c'est d'elles que peut venir une partie de la solution, puisqu'il leur revient de faire appliquer le droit – qui ne semble actuellement pas respecté.

Mme Cyrielle Chatelain, rapporteure. Dans le cadre de votre enquête, avez-vous identifié les clients des *data brokers* ? S'agit-il, par exemple, des grandes centrales publicitaires, comme Google Ads, Meta ou Criteo ?

De même, avez-vous identifié des secteurs dans lesquels les données sont utilisées autrement qu'à des fins publicitaires ? Vous évoquiez notamment la revente de données à des États. Quel est le profil des personnes qui achètent ces données ?

M. Martin Untersinger. Nous n'avons pas obtenu d'informations spécifiques sur les clients des *data brokers*. Les acteurs que vous avez cités se situent plutôt en amont de la chaîne par rapport aux courtiers.

En revanche, ce qu'on sait, et vous venez d'y faire référence, c'est qu'à ce marché foisonnant des données publicitaires s'est greffée une industrie spécifique, qui achète ces données, les consolide, les analyse et les revend. Une partie de ces données sont destinées à la puissance publique, notamment pour l'analyse des flux à l'intérieur des villes, ou aux entreprises privées, pour connaître le cheminement des personnes au sein d'un quartier, afin de voir dans quelles enseignes elles s'arrêtent. Mais surtout, une industrie de la surveillance étatique s'est greffée au secteur publicitaire. Une quinzaine ou une vingtaine de sociétés achètent des données, notamment et vraisemblablement auprès de courtiers, pour fournir des outils de géolocalisation et de pistage à des services de renseignement ou de police.

En l'espèce, la question légale est plus compliquée, car si la collecte de données et leur utilisation en l'absence du consentement de la personne ne sont pas autorisées, leur usage par la puissance publique n'est pas nécessairement illégal, les juristes n'étant pas tous d'accord sur ce point. Quoi qu'il en soit, le marché, lui, est illégal.

Cette industrie ne pose pas les mêmes questions que celle de la surveillance qui vend des logiciels espions intrusifs. Les données publicitaires peuvent d'ailleurs – j'aurais dû l'indiquer plus tôt – être manipulées ou gonflées artificiellement, ce qui altère leur fiabilité. Mais cela reste des outils permettant de géolocaliser, avec des contrôles encore moins importants que ceux qui existent pour d'autres solutions de surveillance étatique.

Il y a par exemple tout un débat sur le fait que l'État américain achète des données révélant des informations qui ne sont normalement accessibles que grâce à un mandat de la justice. Or il considère que ces données préexistent et sont publiques : il les achète donc et les utilise.

Ces pratiques interrogent d'autant plus qu'il n'y a aucune notion de limite géographique. Rien n'empêche un acteur, disons un service de renseignement d'un pays sur lequel j'enquête, d'acheter des données et de me géolocaliser. Cela pose donc question pour les journalistes, les activistes, etc.

Mme Cyrielle Chatelain, rapporteure. La surveillance de masse devient une préoccupation grandissante, notamment aux États-Unis où il y a eu un changement de régime assez important. Hier, Meredith Whittaker témoignait du fait que des discussions sur Facebook avaient été utilisées lors d'un procès contre une femme qui avait aidé sa fille à avorter. Savez-vous si des géolocalisations peuvent être utilisées à des fins de surveillance aux États-Unis, par exemple pour criminaliser l'action d'ONG ou encore l'accès aux droits reproductifs des femmes ?

M. Martin Untersinger. Il ne me revient aucun exemple spécifique. Cependant, il est très largement documenté depuis plusieurs années que certaines agences américaines, comme le DHS (département de la sécurité intérieure des États-Unis) et son unité ICE (service de l'immigration et des douanes), qui est au cœur de l'actualité, ont acheté auprès des sociétés que j'évoquais des outils de surveillance et de pistage. Or tout l'enjeu et toute la sensibilité de ces données, qui sont *a priori* publicitaires, c'est qu'elles nous géolocalisent dans toutes nos activités quotidiennes. Elles peuvent donc révéler ce que le droit européen considère comme des données particulièrement sensibles. Vous avez mentionné les droits des femmes, mais nous pourrions citer la liberté religieuse, l'appartenance syndicale ou le secret médical. Quand vous voyez le déplacement d'une personne dans un centre d'oncologie, par exemple, cela révèle évidemment des informations médicales sensibles. Nous évoluons dans une sorte de matrice qui collecte à tout instant nos données personnelles, si bien que tous nos secrets et tous les aspects les plus sensibles de nos vies sont concernés.

Puisque cette architecture et ces données existent, initialement à des fins publicitaires, il n'est absolument pas surprenant que la conséquence logique de cet écosystème, qu'on a laissé proliférer depuis vingt ans, soit la greffe de sociétés sur ce marché et la revente de solutions de pistage à des États.

M. le président Philippe Latombe. Nous avons aussi abordé la question du chiffrement avec Meredith Whittaker. Cette question agite beaucoup l'Union européenne, dont le projet de « chat control » est en débat au Parlement européen et a suscité des discussions au sein du Parlement français. Quelle est votre opinion sur le chiffrement ?

À cet égard, Mme Whittaker a indiqué que s'il n'y a pas d'accès au contenu chiffré, des métadonnées extraordinairement importantes peuvent néanmoins être récupérées, celles-ci pouvant révéler avec qui vous avez discuté, où vous vous trouviez, quelle antenne a borné, voire donner une géolocalisation plus précise encore grâce au GPS.

M. Martin Untersinger. D'abord, et je pense pouvoir parler au nom de mes confrères, il est nécessaire de dire que les outils de communication sécurisée, dont Signal est un excellent exemple, sont pour nous journalistes, qui traitons parfois de sujets sensibles, une bénédiction. Ils sont absolument nécessaires en ce qu'ils sécurisent notre travail et permettent le respect effectif du droit à la protection des sources.

À titre personnel, j'utilise ces outils des dizaines de fois par jour et il me semble absolument nécessaire de préserver cet acquis, particulièrement à la lumière du contexte aux États-Unis où se situent la plupart des fournisseurs d'outils de communication. Même si la sécurisation n'est pas totale, car le chiffrement ne concerne que les messages en transit, pouvoir échanger de cette manière est indispensable à l'exercice de la profession journalistique.

Quant aux métadonnées, elles sont effectivement très révélatrices et très précises. Je me souviens d'un ancien chef de la NSA, l'Agence nationale de sécurité américaine, qui avait

dit : « Nous tuons des gens en nous basant sur les métadonnées. » Il est donc absolument crucial de les protéger. En effet, le secret des sources, ce n'est pas tant garder confidentiel ce que vous a dit quelqu'un, mais avec qui vous avez discuté. De mon modeste point de vue de journaliste, la protection des métadonnées est donc aussi importante que le chiffrement des messages.

Mme Cyrielle Chatelain, rapporteure. Je reviens à Strava. Auriez-vous pu collecter le même type de données sur d'autres applications ? Pourquoi avoir choisi celle-ci ?

Par ailleurs, quelles applications envoient-elles des données aux *data brokers* ?

M. Sébastien Bourdon. Nous avons travaillé sur Strava, car c'est de très loin l'application sportive la plus populaire en France et à l'international. Il en existe de nombreuses autres, souvent liées à des marques connues telles que Nike, Adidas ou Garmin. Ces plateformes ont des fonctionnalités équivalentes, ou du moins proches de celles de Strava, aussi aurions-nous pu les utiliser, mais elles sont simplement moins populaires.

Les autres applications qui permettraient de trouver des informations sensibles – cela a d'ailleurs déjà été documenté –, sont les applications de rencontres, comme Tinder, Grindr ou Bumble. Leur principe est le même que les applications sportives : voir le profil des autres utilisateurs et utilisatrices dans un certain périmètre et selon certains critères. Or pour être vu par les autres, il faut que votre téléphone, qui agit comme une balise GPS dans votre poche, indique en permanence où vous êtes.

Le média néerlandais *Follow The Money* a publié une enquête – l'an dernier si je ne fais pas erreur – pour laquelle ils avaient réussi à suivre des militaires américains sur différentes bases en Europe grâce à Tinder. L'idée était de créer des comptes qui agiraient comme des balises autour des différentes bases, afin de voir les militaires qui utilisent cette application y apparaître lors de leurs déplacements.

Nous utilisions déjà Strava lorsque, en 2020, nous travaillions sur l'opération Barkhane, mais nous nous étions aussi localisés sur Tinder à Gao, au Mali. La plupart des Maliens n'utilisant pas Tinder, les seuls profils que nous voyions apparaître étaient ceux de militaires français en poste dans cette base. L'application indique si la personne se situe à 1, 2, 3 ou 4 kilomètres, sachant qu'avec un système de triangulation, on peut même obtenir une localisation très précise, à quelques mètres près ; ce n'est pas très compliqué à faire. Et comme il s'agit d'une application de rencontres, les utilisateurs ajoutent nécessairement des informations personnelles : nom, âge, photos, y compris en uniforme ou avec des armes dans le cas des militaires.

S'il est possible de faire cela au Mali, on peut aussi y parvenir en France métropolitaine. Il ne faut que trois clics pour se localiser sur l'île Longue sur Tinder et cela permettrait certainement d'identifier des dizaines, voire des centaines de militaires français.

M. Antoine Schirer. Le design de ces applications a été pensé pour favoriser les échanges entre les gens, pouvoir accéder au profil des autres, etc. Si nous avons utilisé Strava, c'est parce que l'interface est particulièrement propice à cela. Il y a vraiment des brèches béantes qui ont rendu notre travail particulièrement facile, ou du moins assez aisé pour quelqu'un qui a quelques compétences en programmation.

Avant d'être journaliste, j'ai été designer numérique et je pense qu'il ne serait pas très compliqué de configurer l'application de telle manière qu'il soit toujours possible d'enregistrer

ses footings et d'assurer le service aux utilisateurs tout en protégeant mieux leurs données. En deux heures de discussion, je suis convaincu que nous pourrions davantage verrouiller les choses et empêcher ce que nous avons pu faire.

M. Martin Untersinger. En réalité, quasiment toutes les applications sont concernées par la collecte de données publicitaires. La quasi-totalité des applications et des services qu'elles proposent étant gratuits, les outils sont financés par la publicité. Ils embarquent donc des dispositifs pour en afficher et collecter des données afin de les cibler.

Au risque de me répéter, la difficulté vient du fait que la personne qui récupère les données n'est pas nécessairement l'éditeur de l'application. Même quand vous éditez un célèbre site de petites annonces, la régie publicitaire est externalisée. Or c'est cette dernière qui procède à la collecte. De la même manière, les développeurs de petites applications font souvent appel à des services tiers, par exemple pour compter le nombre de visiteurs. Ces briques de construction d'une application sont gratuites et ces services se rémunèrent grâce à la publicité : ils récupèrent des données de géolocalisation qui alimentent le marché.

Certes, l'éditeur d'une application est responsable au premier chef des données de ses utilisateurs, mais pointer tel ou tel outil ne résout pas le problème et n'aide pas à sa compréhension, car ce sont d'autres acteurs, à un niveau inférieur, qui procèdent à la collecte. Et je répète que toutes les applications sont concernées.

Cela vaut d'ailleurs aussi pour l'application du *Monde* – nous l'avons dit dans nos enquêtes. Nous avons trouvé des données issues de l'application de notre journal dans les fichiers du courtier que nous avons sollicité. Nous nous en sommes d'abord réjouis, pensant que nous pourrions ainsi savoir d'où elles venaient et comment elles étaient arrivées là, le journal n'ayant aucun lien technique ou juridique avec le courtier en question. Nous avons multiplié les mises en demeure, mais ce fut finalement impossible de connaître le circuit ! Quand bien même on identifie les applications d'où viennent les données, la responsabilité du détournement est bien en aval.

M. le président Philippe Latombe. Jusqu'à présent, la collecte de données passait par les cookies. Grâce aux évolutions techniques, d'autres modalités de récupération d'informations sont en train d'émerger pour faire de la publicité ciblée. Quelles évolutions voyez-vous arriver ? Y aura-t-il toujours une fuite en avant, avec des alertes de votre part puis l'intervention systématiquement en retard du législateur ? Pour le dire autrement, sommes-nous comme l'équipe d'Italie, qui court après le ballon, ou avons-nous la possibilité de reprendre la main ?

M. Martin Untersinger. Ce qui est certain, c'est que les acteurs de la publicité se montrent très ingénieux pour collecter les données et passer par d'autres biais que les cookies. En l'occurrence, les données publicitaires mobiles s'appuient sur l'identifiant publicitaire – une suite de chiffres et de lettres – propre à chaque téléphone et auquel sont rattachées toutes les données personnelles collectées. Il y a des moyens de déjouer ce fonctionnement : des paramètres de confidentialité permettent de camoufler ou de changer régulièrement cet identifiant. Mais comme toute l'économie numérique est fondée sur la publicité, que la géolocalisation est perçue comme le Graal, ou du moins comme le moyen de cibler les publicités de manière très fine, les acteurs de la publicité proposent des innovations techniques qui font que nous sommes sans cesse dépassés par les évolutions.

M. Vincent Thiébaut (HOR). Je vous remercie pour ces propos très intéressants. Ce que j'en retiens, c'est que la faille est d'abord humaine. Si j'avais la bonne formation et le bon réflexe au moment où j'utilise une application, à plus forte raison si j'exerce un métier sensible, je me poserais la question du partage de mes données.

Pendant que vous parliez, je me suis amusé à sélectionner au hasard une application dans le Google Store. On m'a alors dit que cette application peut partager ma position et des informations personnelles à des tiers, et ainsi de suite. Cela signifie que nous disposons des informations et que le risque est identifié !

Peut-être devons-nous donc nous demander si ces informations sont assez lisibles et compréhensibles. Et je ne parle pas des mises à jour, notamment des politiques de confidentialité, comme celles, très importantes, que nous avons connues lors de l'entrée en vigueur du RGPD. Tout le monde clique sur « oui » sans savoir ce qu'il valide. Outre le fait de courir derrière la technologie par la loi, n'y a-t-il pas un gros travail de pédagogie à faire ?

Je suis vraiment surpris par les exemples que vous avez donnés, qui relèvent de la défaillance humaine. Il me paraît invraisemblable qu'on n'ait pas demandé aux militaires en Opex d'éviter d'utiliser Tinder le temps de l'opération ! C'est pourquoi j'estime que la faille est d'abord humaine avant d'être technologique.

La technologie, on pourra toujours courir après, elle aura toujours un coup d'avance. Il faut donc la bonne information et la bonne formation de l'utilisateur. Que pourrions-nous faire dans ce domaine ?

M. Martin Untersinger. Je laisserai mes confrères répondre sur les données mises en ligne volontairement.

Pour ma part, je suis plutôt en désaccord avec le fait que les choses relèveraient d'une faille humaine. Certes, on peut se passer d'un smartphone, mais c'est tout de même assez compliqué. Je vois que vous en avez un, je présume pour de très bonnes raisons ; pareil pour moi. Or il est humainement impossible de lire les conditions d'utilisation de chacune des applications qu'on utilise et à plus forte raison des 500 entreprises avec lesquelles elles traitent et auxquelles elles fournissent nos données. La question n'est donc, selon moi, pas du tout individuelle, mais dépend de l'écosystème, de l'application du droit et de la responsabilisation des acteurs de ce marché foisonnant et opaque.

On ne peut raisonnablement demander à quelqu'un de connaître exactement les données qui seront collectées, leur cheminement et la manière dont elles seront utilisées, dans la mesure où même les experts, les régulateurs et les informaticiens sont incapables de le faire.

Il est toujours possible, dans les paramétrages, de limiter l'exposition publicitaire, mais j'ai tendance à penser qu'il est insuffisant de faire reposer sans cesse sur l'individu la responsabilité de sa sécurité numérique et de la protection de ses droits fondamentaux, par le biais, en l'espèce, du respect du droit relatif aux données personnelles. C'est trop compliqué et les pouvoirs publics sont aussi là pour protéger le citoyen de la prédation de cette industrie à laquelle, pour ce qui est des données publicitaires, il est impossible de se soustraire.

M. Sébastien Bourdon. Je suis d'accord, monsieur le député, sur la dimension humaine, mais la question est avant tout systémique. Dans notre dernière enquête, c'est bien une personne en particulier qui a permis d'obtenir la position du *Charles-de-Gaulle*, mais il y

a en réalité des milliers de militaires qui font à peu près n'importe quoi sur Strava et sur d'autres applications. Une personne, à un moment T, a cliqué sur sa montre et révélé la position du bâtiment, mais je n'ai aucun doute sur le fait que d'autres, à bord du *Charles-de-Gaulle*, ont, au cours des dernières semaines, fait strictement la même chose.

Pour être tout à fait honnête, nous avions déjà trouvé le porte-avions il y a plusieurs années au cours d'une de nos précédentes enquêtes, lorsque nous cherchions les gardes du corps. En 2024, nous avions su que le *Charles-de-Gaulle* se trouvait au large du Yémen. Nous n'avions pas publié l'information parce que le contexte n'était pas le même et que les positions avaient quelques mois. Mais nous trouvons très régulièrement la position de bâtiments militaires en mer, y compris des sous-marins nucléaires d'attaque. Le problème ne relève donc pas d'une seule personne.

Oui, ce serait évidemment très bien de mieux former et de davantage sensibiliser les militaires – entre autres professions – aux questions numériques. Je rappelle tout de même les échelles : 1 800 personnes se trouvent à bord du *Charles-de-Gaulle* et la France compte 200 000 militaires. Quant au manque de formation et d'habileté numérique, cela ne concerne pas que Strava, ni les dimensions purement opérationnelles. Il faut être lucide sur le fait que l'immense majorité de la population française maîtrise très mal ce qui se passe sur son smartphone, sans parler de fonctionnalités un peu complexes.

Je termine par une anecdote qui, à mon sens, en dit long. Quand, avec Antoine Schirer, nous avons envoyé nos questions à l'Élysée concernant les gardes du corps du président, le chef du GSPR a fait une erreur. Il m'a enlevé de la boucle, mais a cliqué sur « répondre à tous », laissant donc mes collègues en copie. Son message était destiné au service de communication de l'Élysée et il y indiquait, entre autres, qu'il valait mieux des sportifs que des alcooliques. Au-delà des propos en tant que tels, le fait est que ce monsieur a déjà du mal à adresser un mail aux bonnes personnes – cela arrive à tout le monde.

C'est un fait : l'immense majorité de la population ne sait pas utiliser son téléphone et ne regarde jamais les paramètres de confidentialité de son compte Facebook ou Strava. Il faut de l'éducation, mais pas uniquement au sujet de cette application, ni seulement pour les militaires ; le problème est beaucoup plus large.

M. le président Philippe Latombe. Merci beaucoup pour cette anecdote rafraîchissante. Nous suivrons également avec attention la publication de votre prochaine enquête qui, avez-vous dit, est en bouclage.

Je vous remercie de vous être rendus disponibles et de votre liberté de ton. Si vous souhaitez ajouter des éléments ou réagir aux prochaines auditions que nous organiserons, n'hésitez pas à nous fournir une contribution écrite.

La séance s'achève à onze heures trente.

———

Membres présents ou excusés

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

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