N° 623

SÉNAT

SESSION ORDINAIRE DE 2024-2025

Enregistré à la Présidence du Sénat le 14 mai 2025

PROPOSITION DE LOI

*tendant à l'***interdiction** *du* **courtage** *de* **données numériques** *des* **personnes morales** *et* **physiques présentes** *sur le* **territoire français**,

PRÉSENTÉE

Par M. Alexandre BASQUIN, Mme Cathy APOURCEAU-POLY, MM. Jérémy BACCHI, Pierre BARROS, Ian BROSSAT, Mmes Céline BRULIN, Evelyne CORBIÈRE NAMINZO, M. Jean-Pierre CORBISEZ, Mme Cécile CUKIERMAN, M. Fabien GAY, Mme Michelle GRÉAUME, M. Gérard LAHELLEC, Mme Marianne MARGATÉ, MM. Pierre OUZOULIAS, Pascal SAVOLDELLI, Mmes Silvana SILVANI, Marie-Claude VARAILLAS et M. Robert Wienie XOWIE,

Sénateurs et Sénatrices

(Envoyée à la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, sous réserve de la constitution éventuelle d'une commission spéciale dans les conditions prévues par le Règlement.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

Ces trois dernières décennies, le numérique a pris une place de plus en plus importante au sein de nos sociétés. Dématérialisation, réseaux sociaux, intelligence artificielle, plateformes, internet des objets, smartphones… Nous sommes tous concernés.

De nombreux sites web et applications ont vu le jour et nous y laissons, en les consultant, une multitude de données personnelles. Même les applications apparemment les plus innocentes comme la météo, les lampes de poche ou le covoiturage sont contaminées par des dizaines de programmes de captation de données.

Ces données, alors même qu'elles nous appartiennent, sont aujourd'hui fortement capitalisées, monétisées voire revendues aux enchères. La chercheuse américaine Shoshana Zuboff parle ainsi de « capitalisme de surveillance ».

Nos données personnelles sont devenues une mine d'or.

Au point qu'aujourd'hui, des sociétés de courtage, peu connues des consommateurs, les accumulent pour les vendre à des entreprises, à des administrations ou à des gouvernements, à des partis politiques, voire à des particuliers dans certains cas, pour des ciblages publicitaires ou dans le cadre d'élections (souvenons-nous du scandale de Cambridge Analytica). Elles s'enrichissent ainsi, de manière conséquente, sur le dos des usagers.

Les courtiers, appelés également « data brokers », travaillent dans des conditions particulièrement opaques et souvent hors du cadre réglementaire posé par le Règlement général sur la protection des données (RGPD).

En effet, les conditions d'utilisation des données personnelles à des fins publicitaires sont parfois exposées de manière si peu explicite que l'utilisateur donne son consentement, sans réaliser vraiment ce qu'il a accepté. Bien peu d'entre eux ont conscience que leurs données personnelles vont être captées puis exploitées.

La plupart des gens se retrouvent également pris au piège de clauses contractuelles « arrachées » par les conditions générales d'utilisation avec un

système qui pousse à cliquer sur le bouton « J'accepte ». Or, ces clauses permettent la captation des données.

Nous sommes loin du consentement accordé de manière libre, informée et explicite qui devrait être la norme.

Malgré les règles européennes qui imposent une anonymisation des données, les courtiers en données disposent d'informations personnelles : nom, âge, sexe, adresse e-mail, numéro de téléphone, date de naissance, lieu de résidence, centres d'intérêt, habitudes de consommation ou encore niveau d'études, niveau de revenu, etc.

Ce genre d'informations permet aux courtiers en données de placer les usagers dans une catégorie prédéfinie et de revendre leurs profils à tous ceux que cela pourrait intéresser.

De plus, trop souvent, les « data brokers » exploitent la notion d'« intérêt légitime », définie à l'article 6 du RGPD, pour contourner certaines obligations, comme celle de permettre aux utilisateurs de comprendre réellement ce qu'ils autorisent lorsqu'ils acceptent que leurs données soient captées.

Enfin, les amendes infligées aux acteurs du numérique au titre du non-respect du RGPD sont bien peu dissuasives et ne les freinent en rien dans la captation de nos données personnelles.

À titre d'exemple, la Commission nationale de l'informatique et des libertés (CNIL) a prononcé une amende administrative de 75 000 euros à l'encontre de la société de courtage en données Tagadamedia, estimant que les formulaires utilisés par cette société pour collecter les données de prospect ne permettaient pas de recueillir un consentement conforme au RGPD. Et cela n'a rien changé à l'activité des courtiers.

Nous sommes, aujourd'hui, placés dans une situation de subordination et de dépendance face aux géants du numérique et à la cohorte de nouvelles entités dont la seule activité est la vente de nos données numériques. Cette situation risque, d'ailleurs, de s'accentuer avec l'émergence de l'intelligence artificielle.

Ces courtiers peuvent connaître tout de nous.

Et cela dans le moindre détail, comme le souligne une enquête internationale d'un collectif de neuf médias, dite des « data brokers files », publiée le 15 février 2025. Notre identité, notre sexualité, l'adresse précise de notre domicile, nos trajets quotidiens, notre situation familiale, nos

revenus, notre état de santé, nos opinions politiques et religieuses, notre casier judiciaire, nos loisirs, nos achats, etc. Rien n'échappe aux « data brokers », et cela souvent sans notre accord tacite et même, parfois, sans l'accord des applications utilisées.

À cet égard, peut être cité le rapport commun du Comité consultatif national d'éthique (CCNE) et du Comité national pilote d'éthique du numérique (CNPEN) du 9 mai 2023.

Selon ce rapport, dans le champ de la santé, les « data brokers » disposent d'informations personnelles *« issues des traces laissées sur internet, telles que des messages sur les réseaux sociaux ou les forums, mais aussi à travers des applications de santé (IdO, traceurs, capteurs) ou de bien-être (fitness, sport). Cela peut aussi inclure des reçus de commandes de pharmacies en ligne, l'historique de téléconsultation ainsi que d'autres sources d'informations médicales publiques ou non. À cela peuvent s'ajouter des données de localisation et de fréquentation des lieux médicaux (cliniques, hôpitaux) ou de salles de sport. À noter qu'il peut être difficile de tracer l'origine de ces données. »*

Enfin, ils peuvent collecter des informations sur nos activités en ligne mais aussi dans « le monde réel », via des registres publics : bans de mariage, cadastres, licences professionnelles, cartes grises, mais aussi de simples programmes de fidélité en magasin.

Notre vie privée ne l'est plus.

Compilant toutes ces informations, ils les revendent à d'autres entreprises à des fins commerciales. Les informations sur notre état de santé peuvent ainsi être revendues à des compagnies d'assurance maladie qui les utilisent pour déterminer le taux de couverture individualisé.

Certaines fois, la revente des données se fait aux enchères en temps réel (« real-time bidding »). Lorsqu'un encart publicitaire est disponible sur l'écran d'un internaute, l'application diffuse son profil auprès de nombreux annonceurs potentiels. L'encart est ensuite vendu au plus offrant, en quelques millisecondes.

Nous le voyons bien : le modèle économique de ces sociétés de courtage repose uniquement sur la collecte de nos données personnelles et leur vente à des fins lucratives, trop souvent à notre insu.

Certaines ont même industrialisé cette collecte en utilisant des bots (« web scraping »).

À cela s’ajoute l’identifiant publicitaire unique, qui est un fichier individualisé, stocké sur un smartphone, un ordinateur ou une tablette. Il permet d’identifier un individu sur un site internet ou une application. Par la suite, il permet d’analyser le comportement de l’individu et de le reconnaître.

Le « pistage » en ligne est généralisé, facilité par les « cookies », et les courtiers en données contrôlent 95 % des interactions en ligne.

La collecte est massive ; la quantité et la circulation de nos données personnelles sont hors de contrôle.

Il y aurait 4 000 entreprises de courtage de données dans le monde et le marché des « data brokers » représente 400 milliards d’euros en Europe.

Ces entreprises forment un lobby puissant aux objectifs clairs : supprimer la protection de la vie privée en ligne, limiter les réglementations, affaiblir ou bloquer la législation améliorant la confidentialité et contrecarrer toute tentative qui pourrait restreindre leurs pratiques.

Enfin, ce secteur pose des questions majeures d’ordre éthique et moral.

L’enjeu démocratique est réel : ces données accumulées peuvent conduire à des manipulations à grande échelle.

Sans oublier les risques importants liés au vol de ces données par des hackeurs ou encore leur instrumentalisation à des fins politiques, notamment au sein des États autoritaires.

Le législateur se doit de protéger nos données personnelles. La régulation ne suffit malheureusement plus face à ces sociétés prédatrices.

Face à la situation ci-dessus exposée, nous considérons que la protection des données et de la vie privée se fera, en partie, par l’interdiction d’exercice de ces sociétés de courtage en données numériques personnelles.

Proposition de loi tendant à l'interdiction du courtage de données numériques des personnes morales et physiques présentes sur le territoire français

Article 1er

Toute activité de courtage de données consistant à collecter, agréger, traiter, vendre, louer, céder, échanger ou autrement transférer à des tiers des données numériques à caractère personnel ou non personnel est interdite.

Article 2

Cette interdiction s'applique à toute donnée collectée ou traitée dès lors qu'elle concerne des personnes physiques ou morales dont l'adresse IP (Internet Protocol) se trouve sur le territoire national.

Article 3

① Tout contrevenant à la présente loi s'expose à :

② 1° Une amende administrative ne pouvant excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial de la société. Pour les manquements les plus graves, ce montant peut s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial ;

③ 2° Cinq ans d'emprisonnement en application de l'article 226-22-1 du code pénal ;

④ 3° La cessation immédiate des activités prohibées, sous astreinte journalière dont le montant ne peut excéder 100 000 euros par jour de retard ;

⑤ 4° Des peines complémentaires, notamment l'interdiction temporaire ou définitive d'exercer l'activité de traitement de données.

Article 4

La Commission nationale de l'informatique et des libertés est chargée de la mise en œuvre et du contrôle de l'application de la présente loi. Elle dispose de tout pouvoir d'enquête, d'injonction et de sanction nécessaire.

Article 5

L’interdiction mentionnée à l’article 1er entre en vigueur un an après la promulgation de la présente loi.