Fondation Jean Jaurès

Démocratie

L'UTILISATION DES NOUVELLES TECHNOLOGIES PAR LES POUVOIRS PUBLICS

Paula Forteza

01/06/2021

Suite aux travaux menés par la mission d'information de l'Assemblée nationale sur « la guerre des drones » et à la volonté du gouvernement d'étendre l'utilisation des algorithmes dans le cadre de son dernier projet de loi consacré au renseignement, Paula Forteza détaille dans cette note plusieurs exemples et méthodes pour une meilleure utilisation des nouvelles technologies par les pouvoirs publics dans l'avenir.

Le Parlement est une nouvelle fois amené à se prononcer sur un projet de loi relatif au renseignement et à la sécurité intérieure. Une nouvelle fois, la question de l'utilisation des nouvelles technologies par les pouvoirs publics est mise au débat. Une nouvelle fois, nous avançons à l'aveugle.

À chaque fois qu'une nouvelle technologie fait son apparition dans le débat public, elle est présentée comme une « solution miracle ». Il y a un an, TousAntiCovid devait nous permettre de contenir rapidement et efficacement la pandémie. Il y a quelques mois, l'usage extensif de drones était vu comme la solution idoine pour traquer les délinquants et régler les problèmes d'insécurité du quotidien. Aujourd'hui, ce sont les algorithmes de renseignement qui sont présentés comme la technologie indispensable pour nous prémunir d'attaques terroristes.

Dans cette note, je reviens sur l'inflation législative liée aux technologies à risque de ces dernières années. Cette tendance est d'autant plus préoccupante qu'elle a lieu à la va-vite : sans évaluations ni études d'impact sérieuses, sans cadre de réflexion, sans véritable débat démocratique.

Pour appréhender ces sujets, il nous faut adopter une méthode d'analyse sur au moins trois niveaux :

- niveau technique : cette technologie est-elle efficace ?
- niveau juridique : cette technologie fait-elle l'objet de garde-fous suffisants et de

mécanismes de contrôle effectifs ?
- niveau éthique : cette technologie est-elle socialement acceptable ?

Pour chaque niveau, je formule des propositions à-même de renforcer le contrôle démocratique sur l'usage des nouvelles technologies par les pouvoirs publics.

Niveau technique : évaluer l'efficacité de la technologie en question

L'efficacité est la première question que se posent les experts techniques lorsqu'ils développent une nouvelle solution. Deux exemples récents nous permettent d'illustrer ce niveau de réflexion : l'application TousAntiCovid et les algorithmes de surveillance.

Exemple 1 : l'application de *contact-tracing* TousAntiCovid

L'application TousAntiCovid (ex-StopCovid) a fait l'objet d'un débat parlementaire en mai 2020. Cette application est fondée sur la technologie dite de « contact-tracing ».

Pour le Chaos Computer Club, l'acteur de la société civile le plus influent en Europe concernant l'étude des effets des technologies sur la société et les individus, les applications de « contact tracing » sont classées parmi les technologies à risque. Leur déploiement doit être strictement conditionné à leur efficacité : « S'il s'avère que le 'suivi des contacts' *via* l'application n'est pas utile ou ne remplit pas pleinement le but, l'expérience doit être terminée. »

Il apparaissait déjà à l'époque que son efficacité serait toute relative : nous en faisions état avec Baptiste Robert, expert en cybersécurité, le 18 avril 2020 dans une note intitulée « #StopCovid : une efficacité incertaine pour des risques réels« . De par les effets réseaux nécessaires pour son fonctionnement, son efficacité était fonction, notamment, d'un nombre conséquent de téléchargements. Selon une étude de chercheurs de l'université d'Oxford parue en mai 2020, le nombre d'utilisateurs aurait dû se situer à au moins 60% de la population pour que la technologie soit efficace.

Nous avons maintenant un an de recul et savons que cette application n'a jamais fonctionné. Le taux d'adoption et le taux de déclaration très faibles n'ont permis de signaler qu'un nombre marginal de cas au regard du nombre total des cas quotidiens confirmés : au début du mois de novembre 2020, au pic de la seconde vague, l'application ne permettait de notifier que 0,55% des cas contacts, comme le souligne l'expert des données Christian Quest.

Pour rendre l'application efficace, son téléchargement aurait dû être rendu obligatoire, ce qui est inenvisageable en France et contraire au droit européen. Par ailleurs, d'autres États avaient fait le choix, à ce moment-là, d'utiliser d'autres technologies : Israël et la Corée du Sud avaient choisi d'utiliser le « tracking » par GPS, beaucoup plus intrusif puisque ces applications permettaient de suivre en temps réel les déplacements individuels. La Chine et la Russie sont allées encore plus loin en utilisant des technologies de reconnaissance faciale pour contrôler l'application des quarantaines. Ces dispositifs ont certainement une efficacité plus importante. C'est pourquoi il est indispensable d'avoir deux autres niveaux de réflexion : juridique et éthique.

Exemple 2 : les algorithmes de renseignement

Autre exemple d'efficacité questionnable : les algorithmes de renseignement. Le nouveau projet de loi renseignement présenté au Parlement en mai 2021 prévoit de généraliser cette technologie prévue à titre expérimental depuis la loi de 2015. Jusqu'à présent, trois algorithmes ont été mis en place pour capter un large nombre de métadonnées téléphoniques afin d'identifier des signaux faibles. Il peut s'agir de données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communication électronique, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation d'équipements terminaux ou encore à la liste de numéros appelés et appelants, à la durée et à la date des communications.

À ce jour, l'étude d'impact présentée par le gouvernement est très parcellaire du fait de la confidentialité de la technologie appliquée. Nous savons seulement que cette technologie a permis de générer 1739 alertes qui ont conduit à lever l'anonymat. Un rapport parlementaire d'évaluation de la loi de 2015 corrobore ce manque d'informations.

En outre, le projet actuel du gouvernement souhaite étendre ces algorithmes aux URL. Notre droit est très clair sur le type de données qui peut être collecté. Ces informations ou documents ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, ainsi que le précisent les articles L. 851-7 et R. 851-5 du code de la sécurité intérieure et que l'a rappelé le Conseil constitutionnel dans sa décision n° 2015-713 DC du 23 juillet 2015, par laquelle il a jugé que « le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées ».

Dès lors se pose la question de l'efficacité. Nous savons qu'environ 80% du trafic internet est chiffré (*via* le protocole https). Nous savons aussi que les fournisseurs d'accès internet (FAI) n'ont pas le droit de conserver les traces de requêtes. Seuls les hébergeurs de contenus peuvent avoir

des informations suffisamment précises sur les données de connexion. Or, ces hébergeurs sont principalement basés à l'étranger, ce qui rendrait impossible d'y « brancher » des algorithmes. Enfin, se pose la question du traitement de ces données. Nous avons interrogé plusieurs experts qui pointent la nécessité de créer plusieurs dizaines d'emplois uniquement pour pouvoir traiter l'ensemble des données collectées, avant même que celles-ci puissent être exploitables par les services de renseignement.

Ainsi, avant de prévoir leur généralisation, les algorithmes de renseignement devraient faire l'objet d'une évaluation plus approfondie. C'est ce que recommande la CNIL dans ses trois délibérations rendues publiques en avril et mai 2021, déplorant le manque d'information sur les expérimentations en cours et préconisant une expérimentation pour l'extension de cette technologie aux URL.

Proposition 1 : *Donner la capacité au Parlement d'étudier l'efficacité de l'usage des nouvelles technologies*

Pour renforcer le pouvoir des parlementaires dans la compréhension de l'efficacité de ce type de technologies, je propose deux solutions. La première est l'obligation de fournir une étude d'impact sur toute utilisation de nouvelles technologies par les pouvoirs publics sur laquelle le législateur est amené à se prononcer. Le gouvernement n'avait pas eu à fournir d'étude d'impact sur TousAntiCovid, par exemple, puisqu'il s'agissait d'un débat suivi d'un vote et non d'un projet de loi. De même sur la question des drones détaillée ci-après : il s'agissait d'une proposition de loi, n'obligeant pas à recourir à une étude d'impact. Enfin, l'étude d'impact sur les algorithmes de renseignement ne contient que des informations parcellaires : le secret défense devrait pouvoir être levé au moins pour les parlementaires siégeant à la commission saisie au fond.

La seconde solution est de renforcer les capacités du Parlement lui-même concernant ces enjeux, en créant une véritable commission chargée du numérique, dotée d'administrateurs et d'experts en nouvelles technologies. Cette commission pourrait se saisir au fond et pour avis de tous les textes de loi qui concernent le numérique et les nouvelles technologies

Niveau juridique : renforcer les garde-fous et les mécanismes de contrôle

Les technologies déployées par la puissance publique se fondent sur la collecte massive et le traitement approfondi de données personnelles. Sans de solides garde-fous juridiques et des mécanismes de contrôle appropriés, ces technologies représentent des atteintes à la vie privée des personnes qui est protégée par la Constitution.

Deux exemples récents nous permettent de questionner les garanties prévues par le gouvernement : l'usage extensif de drones par la police et la technologie de *scrapping* des données sur les réseaux sociaux pour lutter contre la fraude fiscale.

Exemple 3 : l'usage extensif de drones par la police

L'usage des drones par la police a fait l'objet d'une actualité législative très récente. En l'absence de cadre juridique pour leur utilisation, le Conseil d'État avait sanctionné la préfecture de police de Paris en mai 2020 lorsque cette dernière avait fait voler des drones pour contrôler le respect du confinement.

C'est ainsi que la loi sécurité globale présentée au Parlement en novembre devait créer un cadre clair. Seulement, le cadre proposé était beaucoup trop large et flou. Ainsi, il était initialement prévu une dizaine de cas d'usage des drones. Mis bout à bout, l'ensemble de ces motifs pouvaient conduire à un déploiement de drones en continu.

Lors des débats parlementaires, j'avais proposé de considérer les drones comme des techniques spéciales d'enquête, dont le déploiement est soumis à l'autorisation de l'autorité judiciaire dans le cadre d'une enquête de police ou par le préfet dans le cadre d'une opération de maintien de l'ordre. Ce premier garde-fou devait permettre d'en limiter considérablement les usages, mais surtout de ne conditionner l'utilisation qu'en cas d'interventions de policiers au sol. Je suggérais par exemple de substituer le motif de « prévention d'actes de terrorisme » par « la constatation d'actes terroristes et la poursuite de leurs auteurs ».

Nous avions aussi particulièrement insisté, avec des collègues de plusieurs groupes, pour exclure la possibilité d'exploiter ces données avec un système de reconnaissance faciale. Aucune de ces propositions n'avait été retenue.

En outre, la technologie des drones questionne plusieurs principes fixés par le Règlement général sur la protection des données (RGPD), texte fondamental de notre droit européen sur la protection des données personnelles, et son usage doit de ce fait être strictement encadré notamment au regard de trois principes clés.

Le premier principe est le consentement libre et éclairé au traitement des données personnelles. Avec les drones, il est techniquement impossible de consentir au traitement de nos données personnelles, puisque ceux-ci sont indétectables et mouvants (contrairement à des caméras fixes qui font l'objet d'un signalement). Les citoyens ne peuvent avoir connaissance qu'un drone les

survole. Ainsi, l'obligation d'information du public est extrêmement difficile à remplir. J'avais proposé pendant les débats parlementaires la création d'un registre ouvert avec les données de géolocalisation des vols de drones, ainsi que la possibilité d'un droit individuel d'accès direct aux images *a posteriori* (ce qui est notamment le cas concernant la vidéosurveillance).

Le second est la minimisation de la collecte des données. Avec les drones, nous changeons de paradigme : nous filmons par défaut et non plus par exception ou de manière ciblée. Le recueil exhaustif, préventif et exploratoire (« au cas où ») permis par des cas d'usage trop larges rendait le dispositif complètement disproportionné.

Le troisième principe est l'encadrement particulier des données dites sensibles. Il s'agit d'une catégorie particulière de données personnelles qui comprend les données génétiques, biométriques, de santé, celles relatives à la prétendue origine raciale ou ethnique, à l'opinion politique, religieuse ou encore l'orientation sexuelle. Leur traitement est interdit sauf dans des cas très précis. Ainsi, la proportionnalité dans le recueil de ces données est une nécessité absolue. Par exemple, le texte prévoyait le déploiement de drones pour sécuriser les manifestations, sans autorisation préalable d'une autorité judiciaire ou administrative. Cela ouvrait la possibilité technique d'un profilage massif des personnes en fonction de leurs opinions politiques.

Ces différents points ont conduit le Conseil constitutionnel à censurer le 20 mai dernier une large partie de l'article de loi relatif à l'usage des drones en fonction d'un manque de garde-fous et de contrôles suffisants permettant de protéger la vie privée de nos concitoyens.

Exemple 4 : la surveillance des réseaux sociaux pour lutter contre la fraude fiscale

En novembre 2019, le gouvernement a pris, à titre d'expérimentation, une disposition nouvelle pour lutter contre la fraude fiscale. L'administration des douanes et du fisc peut développer un script de *web scrapping* pour procéder à la collecte et au traitement automatique de l'ensemble du contenu rendu public sur des opérateurs de plateformes en ligne comme Facebook, Le Bon Coin, Airbnb ou encore Blablacar. En clair, l'administration a désormais le pouvoir de collecter automatiquement des données personnelles rendues publiques sur des plateformes afin de détecter des comportements illégaux comme les fausses déclarations d'imposition, la contrebande d'alcool ou de cigarettes, le trafic de drogues, etc.

À première vue, cette technologie semble être frappée au coin du bon sens : elle vise un mobile louable et n'implique pas une extension de la surveillance de données personnelles privées.

Cependant, lors du débat parlementaire, nous avons été plusieurs à signaler que les données personnelles, même si elles ont été rendues publiques volontairement sur une plateforme, restent des données personnelles. Leur protection doit être assurée. D'abord en ce qui concerne la notification et le consentement des utilisateurs à la collecte de leurs données personnelles par l'administration fiscale. Ensuite la durée de l'expérimentation de trois ans aurait pu etre diminuée, alors qu'il s'agit ici d'une technologie à risque, extrêmement intrusive. Celle de la conservation des données a quant à elle bien été diminuée pendant les débats : fixée initialement à un an, elle a été ramenée à trente jours pour les données non pertinentes et à cinq jours pour les données sensibles. Enfin, la question du stockage sécurisé des données a été soulevée : le rapporteur pour avis avait ainsi proposé que ces données ne puissent être confiées à un sous-traitant.

Comme l'indiquait la Cnil à l'époque, cette technologie induit un « changement d'échelle dans l'utilisation de données personnelles ». Elle déplorait d'avoir du rendre son avis dans l'urgence. En effet, sans un encadrement strict, cette technologie pourrait ouvrir la voie au « profilage ». Le profilage est défini à l'article 4 du RGPD. Il s'agit « d'un traitement utilisant les données personnelles d'un individu en vue d'analyser et de prédire son comportement, comme par exemple déterminer ses performances au travail, sa situation financière, sa santé, ses préférences, ses habitudes de vie, etc. ». Le profilage entièrement automatisé, par l'utilisation d'algorithmes qui recueillent des données sur les réseaux sociaux, est interdit au sens de l'article 22 si la décision qui en découle impacte les droits et libertés de la personne.

Proposition 2 : *Créer un mécanisme de transparence et de contrôle citoyen sur l'utilisation des données personnelles par les pouvoirs publics*

La loi informatique et libertés ainsi que le RGPD encadrent l'utilisation des données personnelles. Et ce grâce au consentement libre et éclairé, au droit d'information et au droit d'accès qui permettent à toute personne de connaître quels types de données personnelles sont en la possession d'une administration et l'utilisation qui en est faite. Il peut même s'opposer à leur traitement, « pour des motifs légitimes », sauf dans des cas particuliers, notamment la sécurité publique, la sécurité nationale ou encore la poursuite d'infractions pénales et de leurs auteurs.

Avec le développement de l'identité numérique, nous devons à terme renforcer ces droits.

Pour cela, nous pouvons nous inspirer du modèle estonien pour renforcer le contrôle de chaque citoyen sur le traitement de ses données personnelles par l'État. L'Estonie prévoit l'impossibilité d'utiliser des données biométriques sans le consentement de la personne. Ainsi, le silence d'un citoyen ne signifie pas son consentement explicite et celui-ci peut décider de consentir

partiellement et sous condition à l'utilisation de ses données. Les Estoniens peuvent par ailleurs savoir en temps réel quelle administration utilise leurs données personnelles. Ils peuvent ainsi avoir la possibilité de déposer un recours pour comprendre quel a été le motif de traitement de ses données et engager une procédure s'il considère que ce traitement est abusif. Nous pouvons ainsi passer d'un simple droit d'information et d'accès à un devoir de transparence de la puissance publique sur l'utilisation des données personnelles et une réelle capacité de contrôle par les citoyens.

Ce droit de recours doit être facilité à titre individuel et collectif. Dans le cadre de la loi de transposition du RGPD, j'avais fait adopter un amendement permettant d'étendre les actions de groupe, contre des acteurs privés ou publics, afin de réparer les dommages causés par un manquement à la loi Informatique et libertés. Aujourd'hui, seuls les syndicats, les associations de consommateurs et les associations déclarées depuis cinq ans et ayant comme objet la protection de la vie privée et des données personnelles peuvent exercer ces actions. Il conviendrait de lever ce verrou pour renforcer la capacité d'action de la société civile. Il faut aussi étudier la question du financement de ces actions de groupe, qui n'ont jusqu'à présent que très peu été utilisées.

Niveau éthique : interroger l'acceptabilité sociale des technologies

Avec l'accroissement des capacités techniques vient la responsabilité. Ce n'est pas parce qu'un dispositif devient techniquement possible qu'il faut nécessairement qu'on en fasse usage comme une course en avant non réfléchie, non maîtrisée. Sur cette question, il faut absolument mettre en place une exemplarité des pouvoirs publics. Nous avons sous nos yeux de plus en plus d'exemples « d'effets de cliquet » : une technologie est d'abord développée dans un cadre limité avec des objectifs « louables », puis étendue à d'autres usages beaucoup plus controversés, pour être enfin, rapidement généralisée.

Deux exemples permettent d'illustrer ces dilemmes éthiques : l'usage de la reconnaissance faciale à des fins d'identification dans l'espace public et le développement de technologies dites « sous la peau ».

Exemple 5 : l'usage de la reconnaissance faciale à des fins d'identification dans l'espace public

Que ce soit en France, en Europe ou ailleurs dans le monde, la reconnaissance faciale s'impose de

plus en plus dans les débats. En décembre 2019, nous demandions avec plusieurs députés et acteurs de la société civile un moratoire sur l'utilisation de la reconnaissance faciale à des fins d'identification dans l'espace public, sans le consentement des personnes concernées.

Le gouvernement annonçait alors son intention d'en expérimenter les usages. Le livre blanc de la sécurité intérieure publié en novembre 2020 est très clair sur l'intention du ministère de l'Intérieur : « À l'instar de ce qui se pratique dans plusieurs pays européens, il apparaît hautement souhaitable d'expérimenter la reconnaissance faciale dans les espaces publics, afin de maîtriser techniquement, opérationnellement et juridiquement cette technologie à des fins de protection des Français. »

En France, les expérimentations comme celle menée à Nice ou la proposition de solution d'identité numérique régalienne Alicem ont récemment soulevé de nombreuses questions : si cette innovation ouvre de nouvelles opportunités économiques, commerciales et de sécurité publique, elle pose néanmoins des problèmes d'éthique et d'acceptabilité sociale.

Un premier élément à prendre en compte pour faire la part des choses entre les différents types d'usages, et leur degré de nocivité, est l'existence d'alternatives proposées à l'utilisateur et donc de consentement au dispositif. C'est le cas du système PARAFE aux frontières aéroportuaires, où les citoyens peuvent opter pour un contrôle de passeport en physique.

Il convient aussi de distinguer la reconnaissance faciale à des fins d'authentification, où le système, d'autant plus s'il est « privacy by design » (protecteur de la vie privée par conception), peut ne pas découvrir l'identité de l'utilisateur mais seulement s'assurer qu'il fait partie de ceux ayant droit d'accès à un certain service (c'est le cas d'Alicem), et celle à des fins d'identification, où l'objectif poursuivi est bien celui de découvrir l'identité d'une personne à partir d'une image, potentiellement prise à son insue.

Plusieurs grandes villes américaines comme Oakland, Portland ou San Francisco se sont déjà prononcées pour un moratoire sur ce deuxième cas d'usage, et cela pour de bonnes raisons. D'une part, la reconnaissance faciale n'est pas à ce jour une technologie totalement mûre et possède encore de nombreux défauts techniques : il existe notamment des biais lorsqu'il s'agit des minorités ethniques, des femmes et des jeunes. D'autre part, cette technologie peut engendrer des dérives mettant en danger nos libertés et notre démocratie, comme le démontrent les cas de répression des manifestations à Hongkong ou la surveillance de la minorité ouïghoure par la Chine. Récemment, c'est en Russie que l'utilisation de la reconnaissance faciale a été détournée de son objet initial de mettre en œuvre les quarantaines dans le cadre de la pandémie : elle est désormais

utilisée pour identifier et arrêter les manifestants opposés au régime. Le déploiement d'un système général de reconnaissance faciale peut mettre fin à toute possibilité d'anonymat, allant à l'encontre de notre conception de la liberté de circulation et d'expression.

Exemple 6 : les technologies « sous la peau »

Enfin, autre exemple de développement de nouvelle technologie problématique : celles dites « sous la peau ». La « surveillance sous-la-peau » (*under-the-skin surveillance*) est un concept développé par le philosophe israélien Yuval Noah Harari. À la faveur de la pandémie, le développement de technologies liées à la santé a fortement accéléré et opéré une mutation substantielle : « Jusqu'à présent, lorsque votre doigt touchait l'écran de votre *smartphone* et cliquait sur un lien, le gouvernement voulait savoir exactement sur quoi votre doigt cliquait. Mais avec le coronavirus, le centre d'intérêt change. Maintenant, le gouvernement veut connaître la température de votre doigt et la tension artérielle sous sa peau. »

Un exemple concret a été développé en Chine. La caméra thermique sur téléphone mobile a été utilisée pour prendre la température des habitants et transmettre ces données aux autorités chinoises.

Autre champ d'investigation technologique : le domaine des émotions. Les progrès de la science se portent désormais sur les émotions, leur simulation par la machine mais aussi leur anticipation et leur compréhension. C'est ce que l'on appelle « l'informatique affective » (*affective computing*). Les technologies de détection des émotions peuvent s'appuyer sur la voix (discerner le timbre, la tonalité, le rythme, etc.) mais surtout sur la reconnaissance faciale pour y déceler l'angoisse, le dégoût, la peur, la joie, la tristesse, la surprise. Certaines expériences sont menées pour coupler l'analyse des émotions avec la reconnaissance faciale des automobilistes pour identifier les chauffeurs en colère. D'autres technologies utilisent des signes physiologiques comme les battements du cœur ou la conductance cutanée.

L'une des prochaines étapes pour la protection de nos données sera de protéger ces données émotionnelles, que nous ne contrôlons pas nécessairement et que nous générons sans le vouloir. Elles disent beaucoup de nous et peuvent avoir un intérêt commercial pour des grandes entreprises, mais aussi politique pour des régimes autoritaires afin de renforcer leur pouvoir de contrôle.

Les géants du Net se sont lancés dans la course au développement de technologies neuronales. Les entreprises technologiques, Facebook et Microsoft, ont chacune investi un milliard de dollars

dans des startups en neurotechnologie. L'une de ces startups, la société *Neuralink*, propriété de l'entrepreneur Elon Musk, a tenu une conférence de presse le 25 août 2020, démontrant l'utilisation chez un animal expérimental (un porc) d'une interface cerveau-ordinateur sans fil permettant d'enregistrer l'activité neuronale de l'animal alors qu'il courait dans son écurie. Elon Musk a annoncé que son entreprise avait entamé le processus pour obtenir une autorisation rapide de l'Agence américaine des produits alimentaires et médicamenteux pour implémenter ces interfaces cerveau-ordinateur chez l'homme. L'objectif de cette technologie est clairement affirmé par le fondateur de Tesla : enregistrer des souvenirs personnels en dehors du corps et augmenter intellectuellement les êtres humains sur la base de l'implantation de l'intelligence artificielle dans le cerveau. Le projet transhumaniste de créer un « homme nouveau » augmenté prend forme.

C'est dans cette perspective que certains États commencent à légiférer. Le parlement chilien a récemment décidé de légiférer sur la protection des « neuro-droits ». Cette législation d'avant-garde s'inspire du texte «Quatre priorités éthiques pour les neurotechnologies et l'IA», publié dans la revue *Nature* en 2017, qui recommande vivement d'incorporer des clauses protégeant ces «neuro-droits» dans le droit. À l'initiative du sénateur Guido Girardi, cette loi vise à encadrer deux aspects. Le premier est l'intimité mentale des personnes : les données cérébrales des personnes sont traitées avec une confidentialité comparable à celle des greffes d'organes. Le second est le droit à l'identité et le maintien de l'individualité des personnes.

Proposition 3 : *Engager une réflexion de société sur l'éthique du numérique*

La résolution de ces questions éthiques ne peut pas se décréter ou venir d'en haut. Une vraie réflexion de société doit être engagée. Je propose qu'une convention citoyenne sur les enjeux éthiques du numérique puisse voir le jour, à la manière de celle sur le climat. Le format des conventions citoyennes pour aborder des sujets numériques se développe, à l'image de celle mise en place par la ville de Paris sur le développement de la 5G. Cette convention pourrait par exemple conduire à rédiger une Charte constitutionnelle du numérique qui contiendrait les grands principes liés aux droits et libertés numériques, sous le modèle de celle que nous avions portée de manière transpartisane au Sénat et à l'Assemblée lors des débats sur la révision constitutionnelle de l'été 2018, finalement interrompus.

En s'inspirant des avancées concernant la bioéthique, nous devons installer une réflexion non pas uniquement en matière de droit à la protection des données personnelles mais aussi en matière de dignité humaine. Nous devons faire attention : aujourd'hui trop souvent le label « GDPR compliant » (respectueux du RGPD) fonctionne comme un blanc-seing donné à des technologies qui posent question en termes d'éthique et d'acceptabilité sociale. Les réflexions sur la dignité, en

matière éthique, impliquent la préservation de l'intégrité physique et psychique d'une personne, la défense de son identité, de son intimité et de son estime de soi. Les transformations numériques à l'œuvre donnent le sentiment d'une perte de contrôle sur nos vies, d'une dérégulation complète des cadres sociaux et d'une marginalisation de l'humain. Reprenons le contrôle et la maîtrise de ces évolutions.