Elise Degrave, Chargée de cours à la Faculté de droit de l'UNamur, Chercheuse au Crids et membre de la Commission Nouvelles Technologies et Vie privée LDH

Numérique et démocratie : musclons-nous !

Bien sûr, le numérique apporte des avantages non négligeables aux citoyens et citoyennes. Mais, de manière moins visible, il bouscule aussi les fondements de notre société démocratique. Il convient, à cet égard, de prendre conscience de la situation critique qui pourrait advenir, et d'agir.

Les citoyen·ne·s et l'État doivent se muscler pour éviter que l'on se réveille un jour, un peu groggys, dans une société qui aurait muté en dehors de tout choix démocratique[1]. Plusieurs tendances préoccupantes apparaissent, qui doivent susciter la vigilance.

Tout d'abord, on sait que l'État détient des données nombreuses et importantes au sujet de chacun·e d'entre nous, à propos de notre santé, notre situation fiscale, familiale, professionnelle… C'est nécessaire pour faciliter les démarches administratives des citoyennes et citoyens, notamment. Mais ces données sont particulières puisqu'ils n'ont pas le choix : ils sont obligés de fournir ces données à l'État, dès leur naissance et tout au long de leur vie. L'État doit donc manipuler ces informations avec précaution. Les garde-fous, fixés par une loi adoptée au terme d'un débat démocratique, sont essentiels pour maintenir la confiance des citoyen·ne·s dans l'État. Pourtant, récemment, le législateur a *choisi de faire sauter certaines de ces balises*.

Contrôle de l'utilisation des données

Ainsi, à l'occasion de la mise en place du Règlement général sur la protection des données à caractère personnel (RGPD) il y a bientôt un an, le législateur a supprimé les comités sectoriels, qui étaient des organes de la Commission de la protection de la vie privée chargés de contrôler l'utilisation des données détenues par l'État. Par exemple, c'est grâce à ce contrôle qu'il a toujours été refusé aux entreprises privées d'utiliser le numéro d'identification au Registre national des citoyens, notamment parce que ce numéro propre à chacun·e est aussi le numéro fiscal et le numéro de sécurité sociale. C'est un précieux sésame qui permet l'accès à de nombreuses informations et ne doit donc pas être banalisé. Par ailleurs, les décisions des comités sectoriels étaient publiées, ce qui donnait une certaine transparence aux traitements de données contrôlés. Malheureusement, le contrôle des comités sectoriels a été remplacé par un simple « protocole », c'est-à-dire un document qui doit être rédigé par l'administration qui transfère des données à caractère personnel et l'administration ou l'entreprise qui les reçoit. Le contenu de ce document est laissé à la discrétion des protagonistes et le transfert organisé par ce document ne doit pas être validé par l'Autorité de protection des données[2]. En clair : il va être très difficile de savoir qui transfère quoi à qui, de vérifier la légalité de ces échanges et de dénoncer les abus.

Dans la foulée, par une loi du 25 novembre 2018, le législateur a choisi d'ouvrir le Registre national aux entreprises. Jusqu'ici, le coffre-fort des citoyen·ne·s a été mis à l'abri des nombreuses tentatives du secteur privé de pouvoir y accéder, la loi du 8 août 1983 encadrant strictement l'usage de ces précieuses données. Aujourd'hui, seule une autorisation du Ministre de l'intérieur est nécessaire, qui peut déléguer ce pouvoir à un·e fonctionnaire.

1 À ce sujet, voy. le débat qui a eu lieu à l'Université de Namur le 25 mars 2019 : « Démocratie en question(s) : les GAFAM vont-ils remplacer les États ? » disponible en podcast : www.rtbf.be/lapremiere/article/detail_a-reecouter-democratie-en-question-s-les-gafam-vont-ils-remplacer-les-etats?id=10149566

2 Art. 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Les balises contenues dans la loi sont faibles[3]. Voilà la porte ouverte aux lobbys, à la réutilisation de ces données pour des finalités de marketing, et à la banalisation du numéro d'identification au Registre national avec tous les risques que cela engendre.

Surveillance généralisée

Une deuxième tendance délicate est la *surveillance de masse* qui tend à se généraliser. Dernier exemple en date, la même loi du 25 novembre 2018 impose l'enregistrement des empreintes digitales sur la puce de la carte d'identité électronique. Pourtant, le projet a reçu deux avis défavorables de l'Autorité de protection des données[4], notamment compte tenu des grands risques de failles de sécurité, confirmées par des chercheurs en cryptologie[5]. Au-delà, les balises juridiques n'ont pas été suffisamment débattues. Ce dispositif sera-t-il efficace ? Pour quelles raisons les données seront enregistrées pour une durée de trois mois, et pourquoi ce délai ? Quelles sont les mesures de sécurité qui seront mises en place contre les risques élevés de « hacking » ? Ce sont des questions qui demeurent sans réponse. Le 22 mars 2019, un recours à la Cour constitutionnelle a été introduit par Matthias Dobbelaere-Welvaert, un juriste spécialisé dans la protection de la vie privée. Il reste à espérer que la Cour livre une analyse à la hauteur de l'importance des libertés en jeu.

Un troisième axe inquiétant est celui du *manque de contrôle effectif* des traitements de données. Il y a presqu'un an, le RGPD a fait grand bruit. Au niveau de son contenu, il ne s'agit pourtant que d'une simple évolution de la matière. La révolution viendrait d'une réelle effectivité de ces règles, ce qui suppose notamment qu'on en sanctionne concrètement le non-respect. À cette fin, la Commission de la protection de la vie privée est devenue « Autorité de protection des données », chargée de jouer le rôle de chien de garde de la démocratie, grâce à des pouvoirs renforcés, notamment le pouvoir d'amende. Malheureusement, le gouvernement a décidé d'opérer cette transformation à budget constant et, vu l'ampleur de la matière, il est à craindre que les moyens humains et financiers manquent à cette autorité pour contrôler de manière effective l'ensemble des responsables de traitements.

Protéger le droit à la vie privée

Par ailleurs, le secteur du numérique est opaque, complexe. Il soulève des enjeux qui bien souvent dépassent les citoyens pris individuellement. Dans ce contexte, il est important que des associations bénéficient d'un droit d'action d'intérêt collectif qui leur permette d'agir d'initiative, en leur nom propre, lorsque la loi a été violée. C'est d'autant plus important qu'il n'y a pas toujours, dans ce domaine, une victime identifiée ou identifiable. Le RGPD le permet. Malheureusement, notre législateur a refusé cette opportunité. Il a conditionné l'action en justice des associations au fait d'avoir reçu un mandat d'une personne concernée[6], et ce contre l'avis de la Section de législation du Conseil d'État et de la Commission de la protection de la vie privée.

Ainsi donc, ces derniers mois ont été marqués par des reculs inquiétants pour la protection des libertés citoyennes dans l'univers numérique. Face à cela, il est urgent que l'État se ressaisisse, et retrouve un rôle fort de régulateur et de protecteur, œuvrant dans l'intérêt général.

Au niveau de l'encadrement normatif de la matière, il est à espérer que les prochains législateurs feront preuve d'une compréhension plus fine des enjeux du numérique, de ses avantages mais aussi de ses dangers, et sache définir les balises adéquates et solides tout en refusant, bien évidemment, de supprimer celles qui existaient jusqu'ici. À cette fin, les hommes et femmes politiques gagneraient à se former aux notions de base de cette matière, à acquérir une compréhension minimale des outils

3 P. Havaux, « Le Registre national, 'indic' du privé. La vie privée n'est pas assez protégée », *Le Vif-l'express*, 5 décembre 2018, pp. 32 à 34.
4 APD, avis n° 19/2018 du 20 février 2018 et avis 106/2018 du 17 octobre 2018.
5 www.rtbf.be/info/belgique/detail_des-chercheurs-inquiets-de-la-prochaine-integration-des-empreintes-a-la-carte-d-identite?id=10152853
6 Art. 220 de la loi du 30 juillet 2018 précitée.

technologiques utilisés par l'État et les entreprises. De telles formations ne devraient évidemment pas être dispensées par les entreprises privées qui trouveraient là un intérêt commercial peu compatible avec le bien public vers lequel doivent tendre les élu·e·s de la Nation.

Quant à la mise en œuvre des règles, le RGPD consacre des droits pour les citoyen·ne·s. Mais la plupart d'entre eux existent chez nous depuis 1992. Si l'on a eu l'impression de les découvrir avec le RGPD, c'est parce que jusqu'ici, ils ont été peu revendiqués. C'est une particularité en matière de protection des données à caractère personnel : les gens ont peur, se plaignent, mais n'agissent pas. Or, sans action de la part des personnes concernées, le droit d'accès aux données, le droit à l'oubli numérique, le droit de s'opposer à un traitement illégal, le droit d'obtenir une réparation financière suite à un traitement de données illégal resteront des coquilles vides, comme ils l'ont trop été jusqu'ici.

Même s'ils sont encore trop peu nombreux, des outils en ligne permettent d'accéder à certaines de nos données et de prendre conscience de certaines réalités. Consulter son dossier au Registre national[7], par exemple, permet de vérifier l'exactitude des données enregistrées à notre sujet et de voir quelle institution les a consultées. De manière plus générale, écrire à une administration ou à une entreprise, demander ce qu'ils ont comme données sur nous, pour quelle raison, pour combien de temps encore, d'où proviennent ces données, etc. doit donner lieu à une réponse dans les 30 jours calendrier sans quoi, il est notamment possible de porter plainte à l'Autorité de protection des données qui étudiera le dossier et imposera, le cas échéant, une sanction.

Il est grand temps que le droit à la protection de la vie privée devienne une réalité concrète et un réflexe qui accompagne naturellement le développement des technologies. Le défi est dans les mains, notamment, du législateur qui doit recadrer la situation, mais aussi des citoyens et citoyennes. Car nous avons des droits, exerçons-les !

7 www.ibz.rrn.fgov.be/fr/registre-national/mon-dossier