…la proposition de loi pour la mise en place d'une

CERTIFICATION DE CYBERSÉCURITÉ DES PLATEFORMES NUMÉRIQUES DESTINÉE AU GRAND PUBLIC

Après son examen par la commission des affaires économiques, le Sénat a, sur le rapport de Mme Anne-Catherine Loisier, adopté à l'unanimité, le 22 octobre 2020, la proposition de loi n° 629 (2019-2020) pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public présentée par le sénateur Laurent Lafon.

Le Sénat a :

- adopté l'article 1er en vue de créer un « cyberscore » des solutions numériques (dans une version ajustée par un amendement du Gouvernement) ;
- supprimé, pour des raisons d'ordre juridique, l'article 2, relatif à la prise en compte, dans la commande publique, des impératifs de cybersécurité.

1. LA PRÉOCCUPATION CROISSANTE DE LA SOCIÉTÉ QUANT À LA SÉCURITÉ DES DONNÉES INFORMATIQUES SE HEURTE À UNE INFORMATION LACUNAIRE

A. LA CYBERSÉCURITÉ, CONTREPARTIE INDISPENSABLE À LA NUMÉRISATION DE LA SOCIÉTÉ, DES POUVOIRS PUBLICS ET DE L'ÉCONOMIE.

L'Anssi définit la cybersécurité de façon technique, comme un « *état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de* ***compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles****. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense* ». Il s'agit donc de préserver les données – personnelles[1] ou professionnelles – stockées et les services proposés des diverses menaces techniques[2]. Mais la sécurité des données peut aussi être menacée par des lois à portée extraterritoriale, comme le *Cloud Act* américain.

Pour ceux qui ont la chance d'accéder à des réseaux performants et de maîtriser les outils numériques – on rappellera ici que, fin 2019, la fibre n'était déployée que pour moins de la moitié des locaux de notre territoire, que la 4G est loin d'être généralisée et qu'il est estimé que 13 millions de Français sont éloignés du numérique –, la vie est de plus en plus virtuelle. Le Gouvernement ambitionne de dématérialiser 100 % des 250 démarches les plus utilisées par les citoyens d'ici à mai 2022. La crise de la Covid a amplifié à la fois la fracture mais aussi certains usages numériques : on a ainsi observé une hausse significative des commandes en ligne et des visioconférences, qu'elles soient utilisées à des fins professionnelles ou personnelles[3].

---

[1] *Une donnée personnelle se définit comme toute information se rapportant à une personne physique identifiée ou identifiable.*

[2] *Voir le rapport annuel « État de la menace liée au numérique », Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces.*

[3] *Voir, sur la hausse de la petite criminalité sur internet pendant le confinement, le rapport d'information de MM. Olivier Cadic et Rachel Mazuir, fait au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat, sur le « suivi de la cybermenace pendant la crise sanitaire », juin 2020.*

Les scandales et les failles de sécurité à répétition qui ont pu affecter de grandes entreprises du numérique ont fait un premier travail de sensibilisation de nos concitoyens aux enjeux de cybersécurité : selon un sondage, 90 % des Français considèrent que les données personnelles sont précieuses, qu'elles devraient être davantage protégées et qu'elles sont convoitées par les géants du Net. Cependant, on observe que cette prise de conscience n'amène pas forcément à un changement d'habitudes. Ainsi, de nombreux Français, y compris des organisations institutionnelles, se sont précipités, lors du confinement, sur les solutions de visioconférences les plus faciles à utiliser sans se préoccuper des risques quant à la confidentialité des échanges. Or, en recourant à des plateformes non sécurisées, les consommateurs s'exposent à de nombreux risques : enregistrement vidéo à l'insu des participants, utilisation de la reconnaissance vocale pour attribution pérenne de propos qu'on pense oubliés à l'issue de la conversation, espionnage, manipulation *via deep fake*…

Les **pouvoirs publics sont également la cible de nombreuses attaques, en particulier les collectivités territoriales et le secteur de la santé**. Au-delà des cyberattaques, la question de savoir si les entreprises auxquelles les pouvoirs publics décident de recourir pour opérer certains de leurs services présentent des garanties suffisantes quant à la sécurité des données qu'elles traitent est régulièrement posée, comme l'illustre la polémique relative au contrat passé par l'État avec Microsoft pour prendre en charge la plateforme des données de santé (*Health Data Hub*), qui centralise les données de santé des Français en vue de favoriser la recherche et l'innovation.

Enfin, **les entreprises sont aussi particulièrement exposées aux risques pesant sur la sécurité de leurs données** : selon une enquête de la CPME, en 2019, 40 % des PME déclaraient avoir déjà subi une attaque ou une tentative d'attaque. Selon un sondage, seules 39 % des entreprises se disent suffisamment préparées en cas de cyberattaques de grande ampleur. La question de savoir si les prestataires choisis présentent des garanties suffisantes quant à la sécurité de leurs données stratégiques se pose également pour les entreprises, lesquelles ne sont pas protégées par un règlement général de protection des données, contrairement aux personnes physiques.

B. LES DISPOSITIONS EN VIGUEUR NE GARANTISSENT PAS UN NIVEAU D'INFORMATION SUFFISANT DE L'UTILISATEUR.

Les consommateurs, quant à eux, sont protégés, en tant que personnes physiques, par le règlement général de protection des données adopté au niveau européen en 2016. Celui-ci n'impose cependant pas d'informer sur la cybersécurité des solutions proposées par un prestataire de solutions numériques. Il impose en revanche aux responsables de traitement d'assurer la sécurité des données. Une telle obligation est également imposée à certaines plateformes (places de marché, moteurs de recherche, services *cloud*) par le droit européen de la cybersécurité, lequel prévoit également, à terme, des certifications harmonisées de cybersécurité. Cependant, une telle certification reste une démarche volontaire de l'entreprise concernée. Le droit des communications électroniques impose, enfin, à certains services en ligne des obligations de sécurité. On constate donc qu'**aucune disposition ne garantit l'information du consommateur quant à la sécurité informatique de la solution numérique qu'il utilise**.

S'agissant des marchés publics, aucune disposition n'impose à l'acheteur public de prendre en compte la cybersécurité des solutions proposées. Cela s'explique par la vocation généraliste du code de la commande publique, qui ne comporte pas de dispositions spécifiques aux différentes prestations objets des contrats. Cela ne doit cependant pas empêcher les acheteurs publics de prendre en compte les impératifs qui y sont liés lors de l'achat de fournitures ou de services à travers les marchés publics. La cellule « numérique » de suivi de la crise mise en place par la commission des affaires économiques lors du confinement avait d'ailleurs plaidé pour que la Banque des territoires développe une offre d'ingénierie dédiée à l'accompagnement des collectivités en matière de cybersécurité.

2. MIEUX INFORMER POUR RENOUER AVEC LA CONFIANCE DANS LE NUMÉRIQUE

Afin que les consommateurs et les acheteurs publics prennent davantage en compte les impératifs liés à la cybersécurité, la proposition de loi :

- oblige les plus grands acteurs du numériques à fournir aux consommateurs un diagnostic de cybersécurité afin de mieux les informer sur la sécurisation de leurs données (**article 1er**) ;

- prévoyait que la nature et l'étendue des besoins à satisfaire par un marché public soient déterminés en prenant en compte « *les impératifs de cybersécurité* » (**article 2**).

Partageant pleinement les objectifs poursuivis par la proposition de loi, la commission a estimé qu'il conviendrait de poursuivre la réflexion sur les meilleures modalités d'y répondre et qu'il serait également pertinent de renforcer l'information dont disposent les entreprises.

A. METTRE EN PLACE UN « CYBERSCORE » DES SOLUTIONS NUMÉRIQUES (ARTICLE 1ER).

Le risque pesant sur les usages numériques ne cesse de croître et les utilisateurs sont souvent démunis face aux choix multiples qui s'offrent à eux en matière de services numériques car ils ne bénéficient pas d'une information claire et facile d'accès sur ce sujet. Ils peuvent donc avoir recours, sans le savoir, à des solutions présentant des manques criants en matière de cybersécurité. C'est ainsi que des failles peuvent être exploitées par des acteurs malveillants pour aspirer les données personnelles et les réutiliser.

Afin que le consommateur ne soit plus démuni, **il convient de créer un « nutriscore » de la cybersécurité des solutions numériques, autrement dit « un cyberscore »**. C'est ce que propose l'article 1er. Un tel dispositif bénéficierait également indirectement aux petites structures – associations, TPE, collectivités rurales – en renforçant leur niveau d'information sur les solutions grand public qu'ils sont susceptibles d'utiliser. Ce dispositif reste très largement à construire, c'est pourquoi la proposition de loi renvoie à des textes d'application.

La difficulté résidera sans doute dans la définition des indicateurs pertinents. On peut, par exemple, penser au chiffrement de bout en bout pour les services numériques impliquant des communications. On peut également imaginer des critères de nature moins technique et se rapprochant de la logique de « *name and shame* », comme le nombre de condamnations par une autorité en charge de la protection des données personnelles ou le nombre de failles mises à jour. On peut, encore, imaginer des critères se rapprochant d'une logique de « loi de blocage », en prenant en compte l'existence d'une loi à portée extraterritoriale menaçant les données personnelles.

De plus, on peut s'interroger sur la question de savoir s'il ne serait pas davantage pertinent de ne viser que les données personnelles plutôt que l'ensemble des données.

Un équilibre devrait quoi qu'il en soit être trouvé entre les coûts que ce type d'audit serait susceptible d'engendrer et la nécessité de bien informer le consommateur.

En accord avec l'auteur de la proposition de loi et de son groupe politique, la commission a adopté, à l'initiative de la rapporteure, un amendement (**COM-1**) proposant plusieurs ajustements qu'elle estime susceptibles d'améliorer le dispositif d'un point de vue technique. Il s'agit notamment de ne soumettre que les plus grands acteurs à ce régime d'information, afin d'assurer un équilibre entre innovation et réglementation.

En séance publique, le Sénat a adopté un amendement du Gouvernement (n° 4), sous-amendé par la commission des affaires économiques (n° 6) et par l'auteur de la proposition de loi (n° 7), qui revient principalement à supprimer l'obligation de recourir à un diagnostic *a priori* réalisé par un organisme tiers, au bénéfice, d'une part, d'une auto-évaluation par les acteurs soumis au « cyberscore », d'autre part, d'un contrôle *a posteriori* par les services de l'État (DGCCRF en lien

avec l'Anssi). Lors des débats, la rapporteure et l'auteur de la proposition de loi ont attiré l'attention du Gouvernement sur la nécessité de donner les moyens aux administrations compétentes pour effectuer ces contrôles.

B. GARANTIR LA PRISE EN COMPTE DES ENJEUX DE CYBERSÉCURITÉ PAR LES ACHETEURS PUBLICS (ARTICLE 2).

La commission partage totalement l'objectif poursuivi par cet article, à savoir renforcer la prise en compte des impératifs de cybersécurité dans les marchés publics, et en particulier dans la définition précise du besoin. Deux motifs commandent en effet une telle prise en compte : le premier est de s'assurer que la puissance publique utilise des solutions suffisamment sécurisées et puisse, ainsi, inspirer confiance aux citoyens. Le seconde consiste, dans une logique de politique industrielle, à soutenir les solutions françaises et européennes de confiance et se conformant au règlement général sur la protection des données personnelles, dans un contexte où les États sont très présents dans le soutien aux acteurs concurrents non européens.

Cependant, elle émet des réserves sur le moyen d'atteindre cet objectif proposé par l'article 2, qui se résument de la façon suivante : une loi de portée générale est affaiblie si elle inclut des objectifs particuliers. En effet, les impératifs de cybersécurité ne concernent pas tous les marchés publics. Ce qui emporte deux conséquences :

- en droit, un tel ajout risquerait de se heurter au principe d'égalité devant la commande publique, qui impose de ne formuler les exigences en termes d'expression des besoins, de critères de choix et de clauses d'exécution qu'en lien avec l'objet du marché. Or, une telle exigence portant sur la cybersécurité ne serait pas en lien avec tous les marchés ;

- en opportunité, il est souvent demandé d'ajouter aux articles à portée générale du code de la commande publique des préoccupations légitimes mais particulières, comme la sécurité du travail, l'urgence climatique, la confidentialité, la préservation des données, le bien-être animal… Insérer de telles préoccupations particulières risquerait d'affaiblir la portée de cet article.

Du fait de ces réserves, le Sénat a adopté l'amendement de suppression proposé par le Gouvernement (n° 5).

C. POURSUIVRE LA RÉFLEXION EN VUE D'ACCROÎTRE LA MAÎTRISE DES ENTREPRISES SUR LEURS DONNÉES.

La commission remarque que les entreprises ne sont pas visées par le texte. Or, la sécurisation des données stockées en ligne constitue en effet un enjeu crucial pour la numérisation des entreprises – en particulier des TPE et PME. Elle entend donc mener un travail de réflexion pour aboutir à un dispositif qui pourrait compléter la proposition de loi en ce sens.

La commission rappelle par ailleurs que pour favoriser l'utilisation par les TPE-PME de solutions de cybersécurité, elle avait proposé, lors de l'examen de l'amendement du troisième projet de loi de finances pour 2020, la création d'un crédit d'impôt à la numérisation des entreprises qui aurait pris en compte les dépenses exposées par celles-ci pour assurer leur sécurité informatique. Ce dispositif est cependant à ce jour écarté par le Gouvernement.

Sophie Primas

Présidente de la commission, Sénateur *(Les Républicains)* des Yvelines

Anne-Catherine Loisier

Rapporteur, Sénatrice *(Union Centriste)* de Côte-d'Or

COMMISSION DES AFFAIRES ÉCONOMIQUES

http://www.senat.fr/commission/affaires_economiques/index.html

Téléphone : 01.42.34.23.20

Consulter le dossier législatif :

http://www.senat.fr/dossier-legislatif/ppl19-629.html