N° 38

SÉNAT

SESSION ORDINAIRE DE 2020-2021

Enregistré à la Présidence du Sénat le 13 octobre 2020

RAPPORT

FAIT

au nom de la commission des affaires économiques (1) sur la proposition de loi pour la **mise** *en* **place** *d'une* **certification** *de* **cybersécurité** *des* **plateformes numériques** *destinée au* **grand public***,*

Par Mme Anne-Catherine LOISIER,

Sénatrice

(1) Cette commission est composée de : Mme Sophie Primas*, présidente ;* M. Alain Chatillon, Mme Dominique Estrosi Sassone, M. Patrick Chaize, Mme Viviane Artigalas, M. Franck Montaugé, Mme Anne-Catherine Loisier, MM. Jean-Pierre Moga, Bernard Buis, Fabien Gay, Henri Cabanel, Franck Menonville, Joël Labbé*, vice-présidents ;* MM. Laurent Duplomb, Daniel Laurent, Mme Sylviane Noël, MM. Rémi Cardon, Pierre Louault*, secrétaires ;* M. Serge Babary, Mme Martine Berthet, M. Jean-Baptiste Blanc, Mme Florence Blatrix Contat, MM. Michel Bonnus, Denis Bouad, Yves Bouloux, Jean-Marc Boyer, Alain Cadec, Mme Anne Chain-Larché, M. Patrick Chauvet, Mme Marie-Christine Chauvin, M. Pierre Cuypers, Mmes Françoise Férat, Catherine Fournier, M. Daniel Gremillet, Mme Micheline Jacques, MM. Jean-Marie Janssens, Jean-Baptiste Lemoyne, Mmes Valérie Létard, Marie-Noëlle Lienemann, MM. Claude Malhuret, Serge Merillou, Jean-Jacques Michau, Mme Guylène Pantel, MM. Sebastien Pla, Christian Redon-Sarrazy, Mme Évelyne Renaud-Garabedian, MM. Olivier Rietmann, Daniel Salmon, Mme Patricia Schillinger, MM. Laurent Somon, Jean-Claude Tissot.

Voir les numéros :

Sénat : **629** (2019-2020) et **39** (2020-2021)

SOMMAIRE

Pages

L'ESSENTIEL **5**

I. LA PRÉOCCUPATION CROISSANTE DE LA SOCIÉTÉ QUANT À LA SÉCURITÉ DES DONNÉES INFORMATIQUES SE HEURTE À UNE INFORMATION LACUNAIRE **5**

A. LA CYBERSÉCURITÉ, CONTREPARTIE INDISPENSABLE À LA NUMÉRISATION DE LA SOCIÉTÉ, DES POUVOIRS PUBLICS ET DE L'ÉCONOMIE. 5

B. LES DISPOSITIONS EN VIGUEUR NE GARANTISSENT PAS UN NIVEAU D'INFORMATION SUFFISANT DE L'UTILISATEUR. 6

II. MIEUX INFORMER POUR RENOUER AVEC LA CONFIANCE DANS LE NUMÉRIQUE **7**

A. METTRE EN PLACE UN « CYBERSCORE » DES SOLUTIONS NUMÉRIQUES (ARTICLE 1ER). 7

B. GARANTIR LA PRISE EN COMPTE DES ENJEUX DE CYBERSÉCURITÉ PAR LES ACHETEURS PUBLICS (ARTICLE 2) 9

C. POURSUIVRE LA RÉFLEXION EN VUE D'ACCROÎTRE LA MAÎTRISE DES ENTREPRISES SUR LEURS DONNÉES. 9

EXAMEN DES ARTICLES **11**

- *Article 1er* **Information des consommateurs sur la sécurisation des données hébergées par les plateformes numériques.** 11
- *Article 2* **Prise en compte des impératifs de cybersécurité dans les marchés publics** 21

EXAMEN EN COMMISSION **25**

RÈGLES RELATIVES À L'APPLICATION DE L'ARTICLE 45 DE LA CONSTITUTION ET DE L'ARTICLE 48, ALINÉA 3 DU RÈGLEMENT DU SÉNAT **31**

LISTE DES CONTRIBUTIONS ÉCRITES **33**

LA LOI EN CONSTRUCTION **35**

L'ESSENTIEL

I. 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 extraterritoriales, 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 –, leur 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 numérique 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].

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

---

[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.*

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.

II. 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 plateformes numériques à fournir aux consommateurs un diagnostic de cybersécurité afin de mieux informer ceux-ci sur la sécurisation de leurs données (**article 1er**) ;

– prévoit 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**).

La commission partage pleinement les objectifs poursuivis par la proposition de loi. Elle estime qu'il convient 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 nos 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.

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.

Malgré ces réserves, la commission a adopté l'article sans modification, compte tenu de l'accord entre les groupes politiques relatif à l'examen des propositions de loi.

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 modifiant 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.

EXAMEN DES ARTICLES

Article 1er

Information des consommateurs sur la sécurisation des données hébergées par les plateformes numériques.

Cet article vise à obliger les plateformes numériques à fournir aux consommateurs un diagnostic de cybersécurité afin de mieux informer ceux-ci sur la sécurisation de leurs données.

En accord avec l'auteur de la proposition de loi et de son groupe, la commission a adopté un amendement pour conforter le dispositif proposé.

I. La situation actuelle – La cybersécurité : une exigence croissante, une information des consommateurs lacunaire.

A. La cybersécurité est une menace croissante à mesure de la numérisation de tous les aspects de la vie sociale, ce qui exige une prise de conscience des consommateurs.

1. *La cybsersécurité comme protection des données confiées à un prestataire.*

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 que l'on confie à un prestataire peut aussi être menacée par des lois à portée extraterritoriales. C'est notamment le cas du *Cloud Act* américain, dont la commission d'enquête sur la souveraineté numérique du Sénat a montré les risques. C'est d'ailleurs en raison des législations en vigueur aux États-Unis que la Cour de justice de l'Union européenne a, en juillet dernier, annulé pour la seconde fois l'accord

[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.*

(dit « *Privacy Shield* »[1]) conclu entre l'Union européenne et les États-Unis en vue de permettre le transfert de données personnelles depuis l'Union européenne vers les États-Unis.

La cybersécurité peut donc s'analyser – c'est, à tout le moins, de cette façon que semble l'aborder la proposition de loi commentée – tant au regard d'acteurs malveillants (« pirates » informatiques par exemple) qu'au regard de prestataires qui ne fourniraient pas de garanties suffisantes, soit parce qu'ils ne mettraient pas en place les techniques nécessaires, soit en raison du droit qui s'applique à eux, qui ne serait pas de nature à garantir le respect du droit des données personnelles en vigueur en Europe. Devant la commission d'enquête sénatoriale sur la souveraineté numérique, le directeur général d'OVH rappelait ainsi que « *choisir un acteur américain ou chinois est lourd de conséquences tant au niveau de la protection des données que pour la viabilité à long terme de la filière numérique en Europe* ».

2. *Elle est un risque croissant à mesure que tous les aspects de notre vie sociale se numérise.*

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 –, leur vie est de plus en plus virtuelle : ils interagissent sur les réseaux sociaux, par messagerie en ligne, ils cherchent un emploi et travaillent en ligne, ils remplissent les formulaires administratifs en ligne, ils réservent leurs vacances en ligne, ils écoutent de la musique, regardent des productions audiovisuelles et jouent en ligne, ils s'informent en ligne, etc.

La crise de la Covid-19 a amplifié à la fois la fracture numérique 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.

La croissance à venir de l'internet des objets, qui a déjà été le sujet d'une résolution sénatoriale examinée en 2018 par la commission des affaires économiques[2], est également de nature à étendre la surface de vulnérabilité, comme le prouvent les failles de sécurité régulièrement découvertes dans les enceintes connectées vendues par Amazon et Google.

---

[1] *Cet accord avait été conclu en 2016 suite à l'invalidation du précédent accord (dit* « Safe Harbor »*) par la même Cour.*

[2] *Résolution européenne du Sénat sur la régulation des objets connectés et le développement de l'internet des objets en Europe, mai 2018.*

3. *Si elle semble être une préoccupation essentielle de nos concitoyens, cela ne conduit pas pour autant à une modification des pratiques.*

Dans un sondage réalisé en décembre 2019 pour le compte de la Commission nationale de l'informatique et des libertés (Cnil), l'institut Ifop dévoilait que 68 % des Français se disent plus sensibles qu'avant à la question de la protection de leurs données personnelles[1]. Selon un autre sondage, **plus de 90 % des Français sont d'accord pour considérer que les données personnelles sont précieuses, qu'elles devraient être davantage protégées et qu'elles sont convoitées par les géants du Net**[2].

Cependant, on observe que cette prise de conscience n'amène pas forcément à un changement d'habitudes. Ainsi, selon le sondage Ifop précité, si 45 % des personnes interrogées ont déjà constaté des abus dans l'utilisation faite de leurs données personnelles, parmi elles, **seules 20 % ont pris des mesures en réponse à ces abus**. De même, selon un autre sondage Ifop produit en janvier 2020 pour le compte de la Cnil, 65 % des personnes interrogées donnant leur accord à l'utilisation de leurs données personnelles en ligne **admettent ainsi avoir déjà accepté le dépôt d'un cookie sans en être tout à fait d'accord**, que ce soit par facilité, ou parce qu'ils ne savaient pas comment refuser[3]. Dans le même sens, 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*…

Quoi qu'il en soit, il faut souligner que **plus de la moitié des Français** (56 %) **se disent insatisfaits de l'action des pouvoirs publics**[4]**.**

[1] *Source : rapport annuel de la Cnil pour l'année 2019.*
[2] *Opinion Way pour Dolmen Technologies, Les Français et les scandales liés aux données personnelles, juillet 2019.*
[3] *Source : rapport annuel de la Cnil pour l'année 2019.*
[4] *Sondage OpinionWay précité.*

B. De nombreux textes traitent de la sécurité des solutions numériques, mais ceux-ci ne régissent pas le niveau d'information à donner au consommateur.

Les règles applicables aux solutions numériques – sites internet, logiciels, applications, objets connectés… – constituent un ensemble d'obligations disparates, délicates à articuler entre elles, et ne répondant pas totalement à la problématique de l'information des consommateurs sur les solutions qu'ils utilisent.

1. *Le droit des données personnelles prévoit, sous le contrôle de la Cnil, une certaine information des consommateurs et permettrait l'émergence d'un dispositif de certification volontaire des solutions numériques.*

Des exigences d'information du consommateur mises à la charge de tout responsable de traitement quant aux données personnelles recueillies et à la sécurité des traitements de ces données existent dans le cadre du règlement européen sur la protection des données personnelles[1] de 2016 (dit « RGPD ») « transposé » en France en 2018[2].

Sous peine de sanctions administratives pouvant aller jusqu'à 2 à 4 % du chiffre d'affaires annuel mondial, le responsable de traitement des données doit :

– **fournir certaines informations**, comme l'identité et les coordonnées du responsable du traitement, les finalités du traitement, la durée de conservation des données, les destinataires des données et le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ;

– **mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**. La Cnil a ainsi eu l'occasion de prononcer plusieurs sanctions pour défaut de sécurité[3].

Du reste, le règlement européen prévoit que les États membres « *encouragent (…)* ***la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière****, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent* » ses règles. Ainsi, la Cnil peut, selon la loi française, et dans une logique d'accompagnement des acteurs, « décider de certifier des personnes, des produits, des systèmes de

[1] *Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.*

[2] *Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.*

[3] *Voir notamment la délibération de la formation restreinte n° SAN – 2019-005 du 28 mai 2019 prononçant une sanction pécuniaire à l'encontre de la société SERGIC (sanction de 400 000 euros), délibération de la formation restreinte n° SAN – 2019-007 du 18 juillet 2019 prononçant une sanction pécuniaire à l'encontre de la société ACTIVE ASSURANCES (sanction de 180 000 euros).*

données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement ». Elle n'a, à ce jour, mis en place que la certification des data protection officer. Aussi, on peut s'interroger sur la pertinence, pour l'autorité, de mettre en place une certification des solutions numériques, qu'il s'agisse de sites internet, de logiciels ou d'applications, eu égard à leur cybersécurité dans la mesure où c'est l'Anssi qui, en France, est l'opérateur de la cybersécurité civile. Il convient de noter que la certification est **une démarche volontaire** de l'entreprise concernée.

2. *Le droit de la cybersécurité oblige, sous le contrôle de l'Anssi, certains fournisseurs de services numériques à s'assurer de la sécurité de leurs systèmes d'informations et prévoit un cadre de certification volontaire harmonisé au niveau européen des solutions numériques.*

La directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union de 2016, dite « NIS » transposée en France en 2018[1] impose certaines obligations à certains fournisseurs de service numérique. Trois types de services sont concernés par la directive : place de marché en ligne, moteur de recherche en ligne, service informatique en nuage. Ils sont ainsi tenus de **garantir « *un niveau de sécurité des réseaux et des systèmes d'information nécessaires à la fourniture de leurs services dans l'Union européenne adapté aux risques existants* »**. Ils doivent également notifier les incidents de sécurité affectant les réseaux et systèmes d'information nécessaires à la fourniture de leurs services « *lorsque les informations dont ils disposent font apparaître que ces incidents ont un impact significatif sur la fourniture de ces services* ». Si l'Anssi est informée qu'un fournisseur ne satisfait pas à ses obligations légales, elle est autorisée à procéder à un contrôle, directement ou par l'intermédiaire de prestataires habilités. Elle peut prononcer une injonction administrative et les fournisseurs de services numériques s'exposent à des sanctions pénales en cas d'infraction.

Par ailleurs, le règlement européen relatif à l'Enisa et à la certification de cybersécurité des technologies de l'information et des communications de 2019 (ou *Cybersecurity Act*)[2] prévoit la mise en place d'un **schéma de certification européen** portant notamment sur les fournisseurs de services dits « en nuage ». Ce schéma se substituera aux schémas nationaux des États membres. La certification sera volontaire, sauf disposition contraire du droit de l'Union ou du droit d'un État membre.

En France, l'Anssi propose actuellement deux niveaux de certification.

---

[1] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.*

[2] *Règlement 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013.*

La certification Anssi

Selon l'Anssi, « *la certification est l'attestation du niveau de robustesse d'un produit, basée sur une analyse de conformité et des tests de pénétration réalisés par un évaluateur tiers sous l'autorité de l'ANSSI, selon un schéma et un référentiel adaptés aux besoins de sécurité des utilisateurs et tenant compte des évolutions technologiques* ». Elle se distingue de la qualification, qui est définie comme « *la recommandation par l'État français de produits ou services de cybersécurité éprouvés et approuvés par l'Anssi* ».

Le schéma français offre deux types de certifications, tous deux considérés, comme le souligne l'exposé des motifs de la proposition de loi, « *de haute qualité* » : la **certification « critères communs »**, standard internationalement reconnu s'inscrivant dans des accords de reconnaissance multilatéraux et la « **certification de sécurité de premier niveau** », moins exhaustive en vue de traiter des risques plus modérés. Ces deux certifications sont réalisées par des laboratoires d'analyse technique agréés par l'Anssi.

Les services de visioconférence entrent dans le champ de la qualification appelée « SecNumCloud », gérée par l'Anssi qui permet de certifier l'ensemble des services déployés « en nuage » – c'est notamment le cas de la solution de visioconférence commercialisée par l'entreprise française Tixéo, qui est également certifiée. Les autres cas visés par l'exposé des motifs, comme par exemple les services de stockage de données sur des réseaux privés, pourraient être couverts par la certification de sécurité de premier niveau proposée par l'Anssi.

Ce cadre de certification, qui vise à harmoniser les conditions de la certification par les autorités nationales, est encore en cours d'élaboration au niveau européen, en lien avec les autorités nationales compétentes : selon l'Anssi, l'objectif est de parvenir à un schéma européen au premier semestre 2021 pour une mise en œuvre entre 2022 et 2023. Le schéma de certification devrait comprendre trois niveaux de sécurité, dont le premier niveau avec des coûts de certification limités et l'accès à une information claire et compréhensible pour les utilisateurs finaux.

Par ailleurs, en application du règlement, **des informations devraient être mises à disposition du public par les fournisseurs de produits et services certifiés**, telles que « *des orientations et des recommandations pour aider les utilisateurs finaux à assurer, de façon sécurisée, la configuration, l'installation, le déploiement, le fonctionnement et la maintenance des produits TIC ou services TIC, la période pendant laquelle une assistance en matière de sécurité sera offerte aux utilisateurs finaux, en particulier en ce qui concerne la disponibilité de mises à jour liées à la cybersécurité; les informations de contact du fabricant ou du fournisseur et les méthodes acceptées pour recevoir des informations concernant des vulnérabilités de la part d'utilisateurs finaux et de chercheurs dans le domaine de la sécurité, une mention relative aux répertoires en ligne recensant les vulnérabilités publiquement divulguées liées au produit TIC, service TIC ou processus TIC ainsi que tout conseil pertinent en matière de cybersécurité* ».

3. Le droit des communications électroniques oblige certains fournisseurs de services en ligne à respecter des obligations de sécurité.

Certains services de messagerie en ligne ou de communication par visioconférence pourraient également entrer dans le champ de la réglementation applicable aux communications électroniques issu de la directive portant code européen des communications électroniques adoptée en 2018[1], en tant que « *services de communication interpersonnelle sans numérotation* ».

Les fournisseurs de tels services se voient ainsi imposer une obligation de sécurité, sur le modèle de la directive « NIS », consistant à **prendre « *des mesures techniques et organisationnelles adéquates et proportionnées pour gérer les risques en matière de sécurité des réseaux et des services de manière appropriée* »**. Ils doivent également notifier tout incident de sécurité ayant eu un impact significatif sur le fonctionnement des services. Les États membres doivent veiller à ce que l'autorité compétente pour mettre en œuvre cette disposition ait le pouvoir d'exiger des mesures correctives ou préventives. Les fournisseurs de services doivent également fournir les informations nécessaires à l'évaluation de la sécurité de leurs services à l'autorité compétente et, le cas échéant, se soumettre à un audit.

Dans la transposition envisagée par le Gouvernement dans le cadre de l'ordonnance prévue par le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière actuellement en cours de discussion au Parlement[2] (dit « dadue »), le ministre chargé des communications électroniques devrait être informé en cas d'incident, lequel pourrait enjoindre des mesures pour y remédier. Par ailleurs, l'Autorité de régulation des communications électroniques et des postes (Arcep) pouvant utiliser son pouvoir de sanction en cas de manquement à toute disposition législative ou réglementaire au respect desquelles elle a pour mission de veiller, elle pourrait être saisie pour sanctionner un manquement.

4. Des évolutions en cours.

S'agissant du **droit de la cybersécurité, plusieurs initiatives sont en cours ou à venir au niveau européen**. La Commission européenne prévoit d'adopter une Communication sur la stratégie de cybersécurité le 15 décembre prochain. Le même jour sera présentée une révision de la directive « NIS ».

Le droit de la consommation devrait également bientôt faire une place plus grande aux mises à jour de sécurité : en application de directives européennes que le projet de loi dit « dadue » habilite le Gouvernement à

---

[1] *Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.*

[2] *Projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière, déposé au Sénat en février dernier.*

transposer par ordonnance, les mises à jour de sécurité seront bientôt susceptibles d'être expressément considérées comme des critères de conformité couverts par la garantie de conformité des biens et services numériques[1].

II. Le dispositif envisagé – Une obligation, pour les plateformes, d'informer le consommateur sur la sécurisation de leurs données par la fourniture d'un diagnostic de cybersécurité.

L'**article 1er** de la proposition de loi modifie le code de la consommation en vue d'**imposer aux plateformes d'informer le consommateur sur « *la sécurisation des données* » qu'elles hébergent**, directement ou par un sous-traitant. Concrètement, cette obligation d'information se traduirait **par la fourniture d'un « *diagnostic de cybersécurité* »** dont les indicateurs seraient fixés par décret et qui serait effectué par des organismes également listés par décret, tout comme la durée de validité du diagnostic. Autrement dit, c'est davantage un diagnostic qu'une certification qu'il est proposé de mettre en place.

Article L. 111-7 du code de la consommation, tel que modifié par la proposition de loi

« (…) II.- Tout opérateur de plateforme en ligne est tenu de délivrer au consommateur une information loyale, claire et transparente sur :

1° Les conditions générales d'utilisation du service d'intermédiation qu'il propose et sur les modalités de référencement, de classement et de déréférencement des contenus, des biens ou des services auxquels ce service permet d'accéder ;

2° L'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit, dès lors qu'ils influencent le classement ou le référencement des contenus, des biens ou des services proposés ou mis en ligne ;

3° La qualité de l'annonceur et les droits et obligations des parties en matière civile et fiscale, lorsque des consommateurs sont mis en relation avec des professionnels ou des non-professionnels.

***4° La sécurisation des données hébergées, par l'opérateur lui-même ou ses prestataires. À cette fin, l'opérateur doit fournir un diagnostic de cybersécurité dont les indicateurs sont fixés par décret et effectué par des organismes dont la liste est établie par décret. Sa durée de validité est également fixée par décret**.*

Un décret précise les conditions d'application du présent article en tenant compte de la nature de l'activité des opérateurs de plateforme en ligne. (…) »

En application de l'article L. 131-4 du code de la consommation, tout manquement à ces dispositions serait passible d'une **amende administrative**

[1] *Voir les articles 7 et 8 des directives 2019/771 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens et 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques.*

dont le montant ne peut excéder 75 000 euros pour une personne physique et 375 000 euros pour une personne morale, prononcée par la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF).

L'exposé des motifs précise qu'il s'agit de s'inspirer des diagnostics de performance énergétique imposés en cas d'achat de logement et que cette action s'inscrirait « *dans la continuité du travail déjà réalisé par l'Agence nationale de la sécurité des systèmes d'information (Anssi*) » sur les certifications, bien que le processus devrait, en l'espèce, être moins lourd. L'exposé des motifs précise également que cette proposition « *s'inscrit dans la démarche européenne ayant conduit à la mise en place du* Cybersecurity Act ».

III. La position de la commission – Pour un « cyberscore » des solutions numériques.

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 nos 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. Ce dispositif reste très largement à construire, c'est pourquoi la proposition de loi renvoie abondamment à des textes d'application.

La difficulté résidera sans doute dans la définition des indicateurs pertinents, ceux-ci pouvant être différents en fonction de la solution numérique concernée – site internet, logiciel, application... 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 techniques 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 plus 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.

Ce dispositif se distinguerait de la certification. Il s'agirait de passer d'une logique dans laquelle seul le prestataire qui demande une certification se préoccupe de la cybersécurité de ses solutions, pour accoutumer les consommateurs à ces enjeux et les inciter à se diriger vers les prestataires les plus vertueux.

La certification ne serait nullement remise en cause : elle est également un vecteur efficace pour garantir l'émergence d'une offre de confiance lisible pour les utilisateurs. Ainsi, le « cyberscore » ne viendrait pas perturber la mise en place du schéma de certification au niveau européen : rien ne serait pire que d'avoir à mettre en œuvre une obligation au niveau national sur la base d'un schéma voué à disparaître rapidement (en revanche, une fois un tel schéma volontaire de certification mis en place depuis plusieurs années, l'opportunité de le rendre obligatoire pourrait être envisagée, comme permis par le *Cybersecurity Act* européen) !

En accord avec l'auteur de la proposition de loi et 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 :

– la notion d'opérateur de plateforme, au sens du code de la consommation, dont l'activité consiste en un référencement de produits en ligne ou à la mise en relation de personnes en vue de réaliser des échanges, ne couvrirait pas l'ensemble des solutions évoquées par l'exposé des motifs, notamment le cas des solutions de visioconférence ou des services de stockage en ligne. Il convenait donc d'**adopter une terminologie plus large**, permettant d'embrasser à la fois les sites internet, les logiciels et les applications, embarqués ou non, qu'ils soient à destination du public ou soient le support de correspondances privées. C'est pourquoi la rapporteure propose de recourir à la notion de « *fournisseur de service de communication au public en ligne* » figurant, par exemple, à l'article L. 32 du code des postes et des communications électroniques, qui comprend les services permettant à leurs utilisateurs d'échanger des correspondances et sont soumis, à ce titre, par le même code, au respect du secret des correspondances[1] ;

– afin d'assurer **davantage de souplesse** dans l'établissement et la « mise à jour » des indicateurs, l'amendement substitue au décret définissant les indicateurs et la durée de validité du diagnostic un arrêté et à celui listant les organismes habilités à conduire le diagnostic la désignation de ces organismes par l'Anssi ;

[1] *Article L. 32-3 du code des postes et des communications électroniques.*

– ensuite, l'amendement précise que le diagnostic devrait être **présenté de façon intelligible pour le consommateur** et que cela pourrait se traduire par un logo de type « nutriscore » ;

– enfin, il **limite le champ d'application du dispositif aux services les plus utilisés**, selon des seuils à déterminer par décret.

La commission a adopté l'article ainsi modifié.

Article 2

Prise en compte des impératifs de cybersécurité dans les marchés publics

Cet article vise à modifier le code de la commande publique pour préciser que la nature et l'étendue des besoins à satisfaire par un marché public sont déterminés en prenant en compte « *les impératifs de cybersécurité* ».

Malgré des réserves sur l'opportunité d'une telle insertion, la commission a adopté cet article sans modification en raison de l'accord entre groupes politiques relatif à l'examen des propositions de loi.

I. La situation actuelle – La nécessité d'une attention accrue quant à la sécurité des données traitées par les pouvoirs publics.

A. L'Anssi accompagne des pouvoirs publics particulièrement exposés aux risques cyber.

1. *L'exposition importante des pouvoirs publics aux actes malveillants.*

Comme l'a souligné notre collègue Jérôme Bascher, « *les pouvoirs publics, au cœur des enjeux stratégiques et décisionnels des démocraties, constituent une cible privilégiée des attaquants de toutes origines, étatiques ou non* »[1]. L'Anssi souligne ainsi que, sur la base d'un échantillon d'attaques par rançongiciels[2] en France, « *les collectivités territoriales et le secteur de la santé sont majoritairement concernés (...). Si cela peut être essentiellement dû à la qualité des signalements d'incidents faits à l'ANSSI, cela peut également montrer l'intérêt des attaquants pour des entités réputées faiblement dotées en sécurité informatique ou dont la rupture d'activité aurait un impact social important* »[3].

En effet, en l'absence de ressources humaines adéquates, de nombreuses collectivités se lancent dans le déploiement de solutions

[1] La sécurité informatique des pouvoirs publics, *octobre 2019*.
[2] *Un rançongiciel est un code malveillant empêchant la victime d'accéder au contenu de ses fichiers afin de lui extorquer de l'argent.*
[3] *Anssi,* État de la menace rançongiciel à l'encontre des entreprises et institutions, *2020.*

numériques sans prendre conscience des risques[1]. Selon un sondage, la majorité des fonctionnaires territoriaux estime que leur administration ne possède pas de programme de cybersécurité[2].

2. L'Anssi, acteur de la cybersécurité des pouvoirs publics.

Créée en 2009 dans le sillage du *Livre blanc sur la défense et la sécurité nationale* de 2008, l'Anssi est le principal acteur de l'accompagnement des pouvoirs publics afin de prévenir les risques de cyberattaques, qu'elle agisse dans le cadre du régime des opérateurs d'importance vitale ou au-delà.

Elle concourt à l'élaboration du référentiel général de sécurité auquel les administrations publiques doivent se conformer pour assurer la sécurité des informations échangées par voie électronique avec les usagers[3].

Elle s'est dotée, à compter de 2015, d'un réseau de délégués régionaux pour rapprocher son action des territoires. Elle a publié en janvier 2020 un guide consacré à l'essentiel de la réglementation de cybersécurité à destination des collectivités territoriales.

B. <u>La nécessité de prendre en compte les enjeux de cybersécurité dans les marchés publics.</u>

Deux motifs commandent de prendre en compte la cybersécurité dans les marchés publics. Le premier est de **s'assurer que la puissance publique utilise des solutions suffisamment sécurisées et puisse, ainsi, inspirer confiance aux citoyens**. Plus le degré de sensibilité de la donnée conservée est important, plus la cybersécurité est un enjeu crucial.

Le second 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.

Ainsi, la commission d'enquête sénatoriale sur la souveraineté numérique avait souligné que « *quand les administrations utilisent des logiciels achetés à des entreprises privées, elles doivent s'assurer de la sécurité de l'accès à ces informations et de l'impossibilité pour le fournisseur de les recueillir et de les exploiter* ». Or, elle remarquait que « *lors des auditions menées (…), il ne nous est pas apparu formellement que l'État, dans ses politiques d'achats de matériels et de logiciels informatiques, avait une doctrine générale pour intégrer dans ses appels d'offre cette dimension essentielle de la sécurité des données* »[4]. La polémique

---

[1] *Voir Olivier Kempf,* Cybersécurité et résilience : les grandes oubliées des territoires, *Fondation pour la recherche stratégique, mai 2020.*

[2] *Numerama.com,* Les collectivités territoriales : maillon faible de la cybersécurité du secteur public ?, *7 mars 2018.*

[3] *En application de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.*

[4] Le devoir de souveraineté numérique, *rapport de Gérard Longuet au nom de la commission d'enquête, octobre 2019.*

récente sur le *Health Data Hub*, dont la gestion des données a été confiée à Microsoft, alors que des acteurs français s'estimaient en mesure de réaliser *a minima* une partie du marché, est le dernier épisode en date. Une sénatrice a d'ailleurs demandé la création d'une commission d'enquête[1]. L'affaire fait désormais l'objet d'un contentieux devant le Conseil d'État.

À ce jour, il n'y a **aucune disposition propre à la cybersécurité dans le code de la commande publique**. Cela s'explique par la vocation généraliste d'un tel code, qui traite de l'ensemble de la commande publique, quelle que soit la prestation objet du contrat.

Cela ne doit 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. Ainsi, les acheteurs publics peuvent exiger une certification des solutions numériques qu'ils commandent[2]. Afin d'accompagner les acheteurs publics, un cahier des clauses simplifiées de cybersécurité a été approuvé par arrêté[3].

Du reste, il n'est pas exclu que la responsabilité pénale des personnes publiques puisse être mise en cause pour les dommages causés à autrui par l'intermédiaire d'un système d'information non sécurisé.

II. Le dispositif envisagé – La prise en compte des impératifs de cybersécurité dans la définition des besoins des marchés publics.

L'**article 2** modifie le code de la commande publique pour préciser que **la nature et l'étendue des besoins à satisfaire par un marché public sont déterminés en prenant en compte « *les impératifs de cybersécurité* »**.

Article L. 2111-1 du code de la commande publique, tel que modifié par la proposition de loi

Lors de la préparation d'un marché public, « *la nature et l'étendue des besoins à satisfaire sont déterminées avec précision avant le lancement de la consultation en prenant en compte des objectifs de développement durable dans leurs dimensions économique, sociale et environnementale,* ***ainsi que les impératifs de cybersécurité***. »

L'exposé des motifs souligne l'importance d'adopter « *une réelle stratégie de maîtrise et de protection des données publiques* » compte tenu des attaques quotidiennes contre leurs systèmes d'information, « *qui menacent la continuité du service public et la sécurité des données de nos concitoyens* ».

[1] *Nathalie Goulet, Proposition de résolution tendant à la création d'une commission d'enquête sur la protection des données de santé, juin 2020.*
[2] *Arrêté du 22 mars 2019 fixant la liste des renseignements et des documents pouvant être demandés aux candidats aux marchés publics.*
[3] *Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité.*

III. La position de la commission – Une proposition qui met en lumière les carences des acheteurs publics en matière de cybersécurité.

La rapporteure 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, à la fois pour susciter la confiance du public et soutenir les solutions les plus vertueuses en la matière. Elle rappelle que la cellule « numérique » de suivi de la crise mise en place par la commission des affaires économiques lors du confinement[1] avait plaidé pour que la Banque des territoires développe une offre d'ingénierie dédiée à l'accompagnement des collectivités en matière de cybersécurité.

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, comme l'a souligné auprès de la rapporteure la direction des affaires juridiques des ministères économiques et financiers, 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.

La commission a adopté l'article sans modification, compte tenu de l'accord entre les groupes politiques relatif à l'examen des propositions de loi.

[1] *Anne-Catherine Loisier et Marc Daunis,* Plan de relance de la commission des affaires économiques du Sénat, Tome VII : Numérique, télécoms et postes, *juin 2020.*

EXAMEN EN COMMISSION

Réunie le mardi 13 octobre 2020, la commission a examiné le rapport et le texte de la commission sur 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.

Mme Sophie Primas, présidente. – Nous examinons à présent la proposition de loi, déposée par M. Laurent Lafon, pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public. Il me faut procéder à un rappel concernant la procédure d'examen d'une proposition de loi issue d'un groupe minoritaire. Celle-ci est régie par un accord entre les groupes politiques, dont le principe est le suivant : afin de préserver l'initiative sénatoriale, les groupes minoritaires ont le droit à l'examen de leurs textes, inscrits dans leurs espaces réservés, jusqu'à leur terme, et ces textes ne peuvent être modifiés par la commission sans leur accord. Ainsi, aucun amendement ne peut être adopté aujourd'hui s'il ne reçoit pas l'accord du groupe UC. Bien entendu, des amendements pourront être librement déposés en vue de la séance publique.

Mme Anne-Catherine Loisier, rapporteure. – Vu les délais, j'ai préparé mon rapport sans procéder à des auditions, mais en me fondant sur de rapides consultations écrites.

Cette proposition de loi appelle notre attention sur un sujet crucial, qui monte en puissance mais reste insuffisamment pris en compte par nos concitoyens, qu'il s'agisse des acheteurs publics ou des entreprises : la cybersécurité. La cybersécurité recouvre l'ensemble des dispositifs techniques permettant de préserver la disponibilité, l'intégrité et la confidentialité des données et des services numériques. La sécurité des données peut aussi être menacée par les pratiques des Gafam (*Google, Apple, Facebook, Amazon et Microsoft*), ou par des lois à portée extraterritoriale, comme le *Cloud Act* qui, en 2018, a créé une sorte de droit d'ingérence américain.

Le cyber envahit notre quotidien, en tous cas pour ceux qui ont la chance d'accéder à des réseaux performants et de maîtriser les outils numériques. 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, paradoxalement, à la fois amplifié la fracture numérique et vu exploser certains usages : on a ainsi observé une hausse significative des commandes en ligne et des visioconférences, qu'elles soient utilisées à des fins professionnelles ou personnelles.

Malheureusement, cet usage accru du numérique ne va pas de pair avec les précautions nécessaires. Les scandales et les failles de sécurité à répétition qui ont pu, depuis l'affaire *Cambridge Analytica*, affecter de

grandes entreprises du numérique, ont certes eu un effet 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, cette prise de conscience n'amène pas forcément un changement dans les habitudes de consommation. 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…

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 – ou, il y a quelques années, le recours de la DGSI à *Palantir Technologies*.

Enfin, les entreprises sont aussi particulièrement exposées aux risques pesant sur la sécurité de leurs données : selon une enquête de la Confédération des petites et moyennes entreprises, 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 est donc de savoir si les prestataires choisis présentent des garanties suffisantes quant à la sécurité de leurs données stratégiques, lesquelles ne sont pas protégées par un règlement général de protection des données (RGPD), contrairement à celles des personnes physiques.

La proposition de loi que nous examinons a un double objectif : mieux sensibiliser les consommateurs et les acheteurs publics aux impératifs de la cybersécurité. Elle comporte deux articles. Le premier concerne les consommateurs, le second concerne les acheteurs publics. L'article 1er propose que les consommateurs soient mieux informés sur la sécurisation des données lorsqu'ils utilisent des solutions numériques. De nombreux textes régissent déjà la cybersécurité, à commencer par le RGPD, qui impose aux responsables de traitement d'utiliser des systèmes d'information suffisamment sécurisés. Mais les textes en vigueur sont assez peu tournés vers l'information du consommateur. Cela apparaît comme un vrai manque, que l'article 1er propose de combler. Cela passerait par un diagnostic de cybersécurité obligatoire, dont les modalités exactes sont renvoyées à un décret.

En accord avec M. Laurent Lafon, je vous propose un amendement pour préciser ce dispositif, afin d'en faire un véritable nutriscore de la cybersécurité, autrement dit un cyberscore. Il s'agirait essentiellement d'améliorations d'ordre technique, notamment quant au champ d'application du dispositif, qui ne serait obligatoire que pour les services les plus utilisés et inclurait tous les services numériques, et pas seulement les plateformes au sens du code de la consommation – ce qui permettrait d'inclure les solutions de visioconférence.

L'article 2 propose que les acheteurs publics prennent en compte « les impératifs de cybersécurité » dans la détermination des besoins des marchés publics. Cet article a le mérite d'appeler les acheteurs publics à mieux considérer cet aspect de leurs achats, de plus en plus important, puisqu'on voit se multiplier les applications utilisées par les collectivités territoriales. Il est essentiel d'assurer cette sécurité, à la fois pour garantir la confiance des citoyens dans les services publics numérisés et pour soutenir les acteurs vertueux en la matière.

Cependant, le code de la commande publique a vocation à s'appliquer à tous les marchés publics, et pas seulement à ceux concernés par les enjeux de cybersécurité. Insérer la prise en compte d'un impératif particulier dans un dispositif à vocation générale serait inapproprié et ouvrirait la porte à la prise en compte de nombreux autres impératifs particuliers. Malgré ces réserves, en application de l'accord entre groupes politiques sur les propositions de loi de groupes minoritaires, je ne proposerai pas d'évolution au stade de la commission.

En ce qui concerne les entreprises, qui ne sont pas concernées par la proposition de loi à ce stade, je rappelle que, afin de favoriser l'utilisation, par les TPE-PME, de solutions de cybersécurité, nous avions proposé, avec plusieurs de nos collègues, lors de l'examen d'un amendement au 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. Il mériterait d'être repris.

Au-delà de l'incitation financière des entreprises à se sécuriser informatiquement, et face à la nécessité pour les entreprises de stocker leurs données auprès de prestataires de confiance, je souhaite mener un travail de réflexion pour aboutir à un dispositif d'ici à la séance, qui permettrait de mieux informer les entreprises lorsqu'un prestataire est soumis à une loi extraterritoriale pouvant menacer la sécurité de ses données.

Pour terminer, un point d'ordre technique à propos de l'application de l'article 45 de la Constitution, comme prévu par le vade-mecum applicable en la matière : je vous propose de considérer qu'entrent dans le champ des dispositions présentant un lien direct ou indirect avec le texte les mesures tendant à renforcer l'information du public sur les enjeux de

cybersécurité et de sécurisation des données posés par les services numériques.

En somme, cette proposition de loi arrive très à propos. Je vous proposerai donc de la voter, malgré mes réserves sur l'article 2. En accord avec son auteur et son groupe politique, je proposerai un amendement visant à améliorer l'article 1er.

Mme Sophie Primas, présidente. – Je rappelle que l'article 45 interdit les amendements ne portant pas sur le champ du texte en discussion.

M. Franck Montaugé. – Comment ce texte – dont je partage les objectifs – s'articule-t-il avec le *Cybersecurity Act*, règlement européen datant de 2019 ? L'Agence nationale de sécurité des systèmes d'information (Anssi) propose déjà des certifications de premier niveau. Le texte en tient-il compte ?

Mme Anne-Catherine Loisier, rapporteure. – Nous avons tenu compte du fait qu'un *Cybersecurity Act* doit être mise en œuvre, semble-t-il début 2021. La certification promue par ce texte lui est complémentaire. Surtout, il s'agit de mieux informer le consommateur sur le niveau de sécurité proposé.

M. Franck Montaugé. – Et sur les prestations de l'Anssi ?

Mme Anne-Catherine Loisier, rapporteure. – C'est un domaine différent de celui de l'information du consommateur : il s'agit du dispositif de sécurité demandé par les entreprises dont la vocation première n'est pas d'informer le consommateur. L'Anssi n'est pas oubliée : mon amendement propose qu'elle puisse habiliter les organismes à délivrer les diagnostics de cybersécurité.

M. Franck Montaugé. – J'avais compris que l'Anssi certifiait aussi des processus, outre les organisations d'entreprises. Cela concerne donc les plateformes…

EXAMEN DES ARTICLES

Article 1er

Mme Anne-Catherine Loisier, rapporteure. – Mon unique amendement, COM-1, propose quelques modifications pour compléter et préciser le dispositif. Il étend son champ d'application à tous les services numériques : non seulement les sites internet, logiciels en ligne et autres applications, mais aussi les logiciels de visioconférences – d'ailleurs cités par l'exposé des motifs – ce qui va plus loin que la seule notion de « plateformes en ligne » au sens du code de la consommation. Il limite le champ d'application du dispositif aux services numériques les plus utilisés, selon des seuils à définir. Cela évitera d'imposer de trop fortes contraintes à des petites structures. Il prévoit que la validité du diagnostic soit déterminée par

arrêté, qui aurait vocation à être réexaminé régulièrement. La désignation des organismes habilités à effectuer des diagnostics reviendrait à l'Anssi, qui dispose d'une vision globale sur les dispositifs de cybersécurité, et non à un décret. Enfin, l'amendement précise que le diagnostic devrait être présenté de façon intelligible pour le consommateur et que cela pourrait se traduire par un logo de type nutriscore : c'est l'idée du cyberscore. De cette façon, le consommateur pourrait tout de suite voir s'il fait face à un service sécurisé, moyennement sécurisé ou pas sécurisé du tout.

L'amendement COM-1 est adopté.

L'article 1er est adopté dans la rédaction issue des travaux de la commission.

Article 2

L'article 2 est adopté sans modification.

La commission adopte le texte de la proposition de loi dans la rédaction issue de ses travaux.

RÈGLES RELATIVES À L'APPLICATION DE L'ARTICLE 45 DE LA CONSTITUTION ET DE L'ARTICLE 48, ALINÉA 3 DU RÈGLEMENT DU SÉNAT

Si le premier alinéa de l'article 45 de la Constitution, depuis la révision du 23 juillet 2008, dispose que « tout amendement est recevable en première lecture dès lors qu'il présente un lien, même indirect, avec le texte déposé ou transmis », le Conseil constitutionnel estime que cette mention a eu pour effet de consolider, dans la Constitution, sa jurisprudence antérieure, reposant en particulier sur « la nécessité pour un amendement de ne pas être dépourvu de tout lien avec l'objet du texte déposé sur le bureau de la première assemblée saisie »[1].

De jurisprudence constante et en dépit de la mention du texte « transmis » dans la Constitution, le Conseil constitutionnel apprécie ainsi l'existence du lien par rapport au contenu précis des dispositions du texte initial, déposé sur le bureau de la première assemblée saisie[2]. Pour les lois ordinaires, le seul critère d'analyse est le lien matériel entre le texte initial et l'amendement, la modification de l'intitulé au cours de la navette restant sans effet sur la présence de « cavaliers » dans le texte[3]. Pour les lois organiques, le Conseil constitutionnel considère comme un « cavalier » toute disposition organique prise sur un fondement constitutionnel différent de celui sur lequel a été pris le texte initial[4].

En application des articles 28 *ter* et 48 du Règlement du Sénat, il revient à la commission saisie au fond de se prononcer sur les irrecevabilités résultant de l'article 45 de la Constitution, étant précisé que le Conseil constitutionnel les soulève d'office lorsqu'il est saisi d'un texte de loi avant sa promulgation.

---

[1] Cf. *commentaire de la décision n° 2010-617 DC du 9 novembre 2010 - Loi portant réforme des retraites.*

[2] Cf. *par exemple les décisions n° 2015-719 DC du 13 août 2015 - Loi portant adaptation de la procédure pénale au droit de l'Union européenne et n° 2016-738 DC du 10 novembre 2016 - Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias.*

[3] *Décision n° 2007-546 DC du 25 janvier 2007 - Loi ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique.*

[4] *Décision n° 2011-637 DC du 28 juillet 2011 - Loi organique relative au fonctionnement des institutions de la Polynésie française, confirmée par les décisions n° 2016-732 DC du 28 juillet 2016 - Loi organique relative aux garanties statutaires, aux obligations déontologiques et au recrutement des magistrats ainsi qu'au Conseil supérieur de la magistrature, et n° 2017-753 DC du 8 septembre 2017 - Loi organique pour la confiance dans la vie politique, qui considèrent comme un « cavalier organique » toute disposition organique prise sur un fondement constitutionnel différent de celui sur lequel a été pris le texte initial.*

Lors de sa réunion du mardi 13 octobre 2020, la commission des affaires économiques a arrêté le périmètre de la proposition de loi pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public enregistrée à la présidence du Sénat le 15 juillet 2020 comme suit : les mesures tendant à renforcer l'information du public sur les enjeux de cybersécurité et de sécurisation des données posés par les services numériques.

LISTE DES CONTRIBUTIONS ÉCRITES

– Agence nationale de la sécurité des systèmes d'information (Anssi)

– Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)

– Direction des affaires juridiques des ministères économiques et financiers

– Tech in France

LA LOI EN CONSTRUCTION

Pour naviguer dans les rédactions successives du texte, visualiser les apports de chaque assemblée, comprendre les impacts sur le droit en vigueur, le tableau synoptique de la loi en construction est disponible sur le site du Sénat à l'adresse suivante :

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