N° 503

SÉNAT

SESSION ORDINAIRE DE 2021-2022

Enregistré à la Présidence du Sénat le 16 février 2022

RAPPORT

FAIT

au nom de la commission des affaires économiques (1) sur la proposition de loi, modifiée par l'Assemblée nationale, 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 ;* MM. Serge Babary, Jean-Pierre Bansard, Mmes Martine Berthet, 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 Marie Evrard, Françoise Férat, Amel Gacquerre, M. Daniel Gremillet, Mme Micheline Jacques, M. Jean-Marie Janssens, Mmes Valérie Létard, Marie-Noëlle Lienemann, MM. Claude Malhuret, Serge Mérillou, 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 : Première lecture : **629** (2019-2020), **38**, **39** et T.A. **8** (2020-2021)
Deuxième lecture : **226** et **504** (2021-2022)

Assemblée nationale (**15**ème législ.) : Première lecture : **3473**, **4700** et T.A. **710**

SOMMAIRE

Pages

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 EST UNE 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 de diverses menaces techniques les données professionnelles et à caractère personnel stockées et les services qui leur sont associés. Mais la sécurité des données peut aussi être menacée par des lois à portée extraterritoriale, comme le *Cloud Act* américain.

La question de la sécurisation des données est d'autant plus importante qu'aujourd'hui notre 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, avec par exemple une hausse significative des commandes en ligne et des visioconférences.

Les scandales et les failles de sécurité à répétition qui ont pu affecter de grandes entreprises du numérique, les pouvoirs publics et les collectivités territoriales ont fait un premier travail de sensibilisation aux enjeux de cybersécurité. Les entreprises sont particulièrement exposées aux risques pesant sur la sécurité de leurs données.

Des entreprises déclarant avoir subi au moins une cyberattaque en 2021

Des cyberattaques ont conduit à des vols de données personnelles, stratégiques ou techniques

Des entreprises considèrent la sensibilisation aux enjeux de cybersécurité comme une priorité[1]

Cependant, cette prise de conscience n'amène pas forcément à un changement d'habitudes de consommation : c'est tout l'objet de cette proposition de loi.

B. LES DISPOSITIONS EN VIGUEUR NE GARANTISSENT PAS UN NIVEAU D'INFORMATION SUFFISANT DES CONSOMMATEURS

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 le niveau de 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.

Aujourd'hui, 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

[1] *Données issues du baromètre 2022 sur la cybersécurité des entreprises du CESIN.*

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. UNE MEILLEURE INFORMATION DES CONSOMMATEURS EST INDISPENSABLE 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 initiale :

- oblige les plus grands acteurs du numérique 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**).

A. LA COMMISSION A SOUHAITÉ METTRE EN PLACE UN VÉRITABLE « CYBERSCORE » DES SOLUTIONS NUMÉRIQUES

Alors que le risque pesant sur les usages numériques ne cesse de croître, 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.

Il est donc nécessaire de créer un « nutriscore » de la cybersécurité des solutions numériques, autrement dit « un cyberscore ». Un tel dispositif bénéficierait directement aux consommateurs, mais également indirectement aux petites structures telles que des associations, des TPE et collectivités rurales en renforçant leur niveau d'information sur les solutions grand public qu'ils sont susceptibles d'utiliser.

La délimitation du périmètre d'application est le premier enjeu pour la mise en œuvre d'un tel dispositif. La commission des affaires économiques du Sénat avait élargi le périmètre initial, limité aux opérateurs de plateforme en ligne, pour y intégrer les logiciels de visioconférence. Conformément à cette volonté, l'Assemblée nationale a précisé la rédaction pour inclure de tels logiciels et les systèmes de messagerie instantanée dans le champ d'application du dispositif.

La difficulté résidera sans doute dans la définition, par voie réglementaire, des seuils au-delà desquels les opérateurs de plateformes en ligne et les entreprises seront concernés. La commission souhaite que, dans un premier temps, seuls les acteurs numériques les plus importants soient concernés, afin de ne pas décourager l'innovation des plus petites entreprises proposant des services en ligne. Il s'agit de trouver un équilibre entre innovation et réglementation.

Le deuxième enjeu pour la mise en œuvre d'un tel dispositif concerne sa dénomination et sa nature. Au Sénat, la notion de diagnostic de cybersécurité avait été retenue, l'objectif étant que le dispositif ne soit pas trop contraignant ni trop coûteux pour les opérateurs économiques. À l'Assemblée nationale, c'est finalement la notion d'**audit de cybersécurité** qui a été choisie. Cet audit devra être réalisé par des prestataires agréés par l'Agence nationale de la sécurité des systèmes d'information (Anssi) et portera sur **la sécurisation et la localisation des données**.

Le troisième enjeu concerne le contenu de cet audit de cybersécurité, qui sera défini par arrêté ministériel. Si le critère de localisation des données ajouté par l'Assemblée nationale est important, car déterminant le régime juridique applicable en matière de protection des données et participant de l'affirmation d'une plus grande souveraineté numérique, cela ne peut pas être le seul critère pris en compte pour déterminer la sécurité de l'hébergement des données.

La difficulté résidera dans la **définition des autres indicateurs pertinents** pour réaliser cet audit. La commission estime que des critères techniques pourraient être retenus, comme le chiffrement de bout en bout pour les services numériques impliquant des communications. D'autres critères, moins techniques, pourraient également être envisagés comme le nombre de condamnations par une autorité chargée de la protection des données à caractère personnel ou le nombre de failles mises à jour. L'existence d'une loi à portée extraterritoriale pourrait aussi être prise en compte.

Enfin, le dernier enjeu concerne les modalités d'information des consommateurs. Au Sénat, il a été précisé que le dispositif devait être présenté de façon lisible, claire et compréhensible à l'aide d'un système coloriel. L'Assemblée nationale a maintenu l'ensemble de ces dispositions.

B. LA PRISE EN COMPTE DES ENJEUX DE CYBERSÉCURITÉ PAR LES ACHETEURS PUBLICS N'EST PAS OPPORTUNE DANS CE TEXTE

La commission partage l'objectif poursuivi par cet article, à savoir renforcer la prise en compte des impératifs de cybersécurité dans les marchés publics. 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 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.

Cependant, la commission a émis des réserves sur le moyen d'atteindre l'objectif proposé. En effet, une loi de portée générale est affaiblie si elle inclut des objectifs particuliers. Or, 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 des exigences qu'en lien avec l'objet du marché ;
- 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 ou la préservation des données.

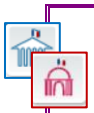
Du fait de ces réserves, **le Sénat a adopté l'amendement de suppression proposé par le Gouvernement en séance publique. L'Assemblée nationale a voté la suppression conforme de cet article**, partageant les mêmes réserves que celles formulées par la commission.

EN SÉANCE

En séance, le Sénat a adopté :

- un amendement du Gouvernement pour élargir le périmètre d'application du dispositif aux principaux opérateurs de plateformes en ligne, sous-amendé par la rapporteure dans l'objectif d'intégrer les systèmes de visioconférence, et sous-amendé par l'auteur du texte pour rendre obligatoire la présentation du « Cyberscore » sous forme de système d'information colorielle ;

- un amendement du Gouvernement pour supprimer l'article 2.



LA SUITE DE LA NAVETTE

À l'issue de l'examen en première lecture à l'Assemblée nationale, il a été adopté :

- un amendement de la majorité pour que les seuils au-delà desquels les acteurs économiques sont concernés par le dispositif soient définis par voie réglementaire et pour qualifier le dispositif d'audit de cybersécurité ;

- un amendement du rapporteur pour que la localisation des données hébergées soit prise en compte par l'audit de cybersécurité ;

- un amendement du rapporteur pour que des prestataires agréés de l'Anssi réalisent cet audit.

En deuxième lecture, le texte a été voté conforme par la commission des affaires économiques du Sénat.

EXAMEN DES ARTICLES

Article 1er (non modifié)

Création d'une certification de cybersécurité des plateformes numériques destinée au grand public

Cet article vise à créer une certification de cybersécurité des plateformes numériques, des services de messagerie et des logiciels de visioconférence à destination du grand public.

La commission a adopté l'article 1er sans modification.

I. Le dispositif initial – Un diagnostic de cybersécurité aux contours encore imprécis

L'article 1er modifiait l'article L. 111-7 du Code de la consommation pour compléter les **informations que les opérateurs de plateformes en ligne doivent fournir aux consommateurs** de façon claire, loyale et transparente afin d'y inclure les informations relatives à la sécurisation des données hébergées.

À cette fin, les opérateurs doivent élaborer un « **diagnostic de cybersécurité** ». Un tel diagnostic s'apparenterait, selon l'exposé des motifs de la proposition de loi initiale, aux diagnostics de performance énergétique qui visent à informer les propriétaires, les locataires et les acheteurs sur la performance énergétique et environnementale des logements.

Toutefois, **les contours et le contenu de ce diagnostic ne sont pas esquissés dans la proposition de loi**, qui renvoie à un décret la détermination des indicateurs utilisés pour élaborer ce diagnostic, la liste des organismes habilités à le faire ainsi que sa durée de validité.

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

II. La position du Sénat en première lecture – La mise en place d'un « Cyberscore » pour faciliter l'information des consommateurs

La commission constate que le risque pesant sur les usages numériques ne cesse de croître, mais que 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.

Afin que le consommateur ne soit plus démuni, **la commission a souhaité créer un « Nutriscore » de la cybersécurité des solutions numériques, autrement dit un « Cyberscore »**.

Toutefois, ce dispositif reste largement à construire. **La difficulté réside dans la définition des indicateurs pertinents**, ceux-ci pouvant être différents en fonction de la solution numérique concernée. Parmi les indicateurs envisagés par la commission, il y a des indicateurs :

- de nature technique, comme le chiffrement de bout en bout pour les services numériques impliquant des communications ;
- de nature moins technique, comme le nombre de condamnations par une autorité chargée de la protection des données à caractère personnel ou le nombre de failles logicielles mises à jour ;
- de nature juridique, comme l'existence d'une loi à portée extraterritoriale menaçant la protection des données à caractère personnel des utilisateurs.

La commission considère également qu'un **équilibre devrait être trouvé entre les coûts de mise en place d'un tel dispositif et la nécessité de bien informer les consommateurs**.

Au regard de ces premières considérations, la commission a adopté, en accord avec l'auteur de la proposition de loi et de son groupe politique, un amendement de la rapporteure proposant plusieurs ajustements susceptibles d'améliorer le dispositif d'un point de vue technique.

Sur le périmètre d'application du dispositif, la commission estime que la notion d'opérateurs de plateforme en ligne, au sens du code de la consommation, ne correspond pas entièrement à la volonté de départ ayant motivé cette proposition de loi. Selon l'exposé des motifs, l'objectif est d'intégrer plusieurs solutions numériques, dont les logiciels de visioconférence ou les services de stockage en ligne.

L'amendement de la rapporteure substitue la notion de « **fournisseur de service de communication au public en ligne** » au sens de l'article L. 32 du code des postes et des communications électroniques (CPCE) à celle « d'opérateurs de plateforme en ligne », notamment **dans l'intention d'inclure les systèmes de visioconférence**.

Sur la souplesse du dispositif, l'amendement de la rapporteure substitue également au décret définissant les indicateurs et la durée de validité du diagnostic un arrêté ministériel et prévoit une désignation des organismes habilités à réaliser un tel diagnostic par **l'Agence nationale de la sécurité des systèmes d'information (ANSSI)**.

Sur l'information des consommateurs, l'amendement de la rapporteure précise que le diagnostic devra être **présenté de façon intelligible pour le consommateur**.

En séance publique, le Sénat a précisé les contours du dispositif de « Cyberscore » en adoptant :

- un amendement du Gouvernement pour préciser que **seuls les opérateurs de plateforme en ligne les plus importants sont concernés par le dispositif, un décret devant définir les seuils au-delà desquels ces opérateurs sont concernés**, dont un seuil de nombre de connexions ;
- un sous-amendement de la rapporteure pour substituer la notion de fournisseurs de service de communication au public en ligne à celle d'opérateurs de plateforme en ligne ;
- un sous-amendement de l'auteur de la proposition de loi pour **rendre obligatoire la présentation du diagnostic de cybersécurité à l'aide d'un système d'information coloriel** lors de la première connexion à chaque service concerné.

III. Les modifications apportées par l'Assemblée nationale – La précision de la délimitation du « Cyberscore »

En commission des affaires économiques, deux amendements du rapporteur ont été adoptés :

- un amendement pour préciser que seuls les opérateurs de plateforme en ligne qui ont au moins cinq millions de visiteurs uniques par mois sont concernés par ce nouveau régime d'information et pour **intégrer explicitement les logiciels de visioconférence et les systèmes de messagerie instantanée dans le périmètre** ;
- un amendement pour transformer le dispositif en véritable **« certification de cybersécurité »** délivrée par des organismes habilités par l'ANSSI.

En séance publique, la délimitation du dispositif et ses modalités d'application ont de nouveau été modifiées, avec l'adoption de plusieurs amendements du rapporteur identiques à ceux déposés par les députés membres du groupe majoritaire :

- un amendement pour **finalement supprimer la référence au seuil de connexion** et la nécessité d'avoir au moins cinq millions de visiteurs

par mois, **pour finalement renvoyer à un décret la définition des seuils d'activité** au-delà desquels les entreprises seront concernées et pour finalement **substituer la dénomination « d'audit » à celle de « certification »** ;

- un amendement pour préciser que l'audit de cybersécurité sera réalisé par des **prestataires agréés par l'ANSSI** ;
- un amendement pour supprimer la présentation de l'audit lors de la première connexion à chaque service concerné mais maintenant le principe d'une information lisible, claire et compréhensible à l'aide d'un système coloriel.

En séance publique également, un amendement du rapporteur a été adopté contre l'avis du Gouvernement, précisant que **l'audit de cybersécurité devra porter sur la sécurisation et la localisation des données hébergées**.

IV. La position de la commission – L'adoption conforme du texte voté par l'Assemblée nationale

Sur le périmètre d'application, l'objectif principal du Sénat est d'avoir un dispositif qui, dans un premier temps, s'applique seulement aux plus grands acteurs et intègre les logiciels de visioconférence, dont l'utilisation s'est généralisée depuis le début de la crise sanitaire.

Après plusieurs modifications et de nombreuses hésitations du Gouvernement, c'est la notion d'opérateurs de plateforme en ligne qui a finalement été retenue par l'Assemblée nationale, mais les systèmes de messagerie instantanée et de visioconférence ont été explicitement inclus, conformément au souhait initial du Sénat.

Un décret d'application devra définir les seuils d'activité au-delà desquels les acteurs économiques seront concernés, dans la même logique que les dispositions adoptées par la commission des affaires économiques du Sénat.

Sur la nature et la dénomination du dispositif, l'objectif principal du Sénat est de permettre la création d'un dispositif d'information qui ne soit pas trop contraignant ou ni trop coûteux.

Il s'agit de trouver un équilibre entre réglementation et innovation et de ne pas pénaliser les TPE, les PME et les start-up innovantes en matière de services en ligne. Ainsi, la notion finalement retenue « d'audit de cybersécurité » se rapproche davantage de ce que la commission entendait par « diagnostic », au contraire de la notion de « certification ».

Sur le contenu de l'audit de cybersécurité, il doit toujours être déterminé par voie réglementaire.

La précision selon laquelle cet audit doit porter sur la sécurisation et la localisation des données est importante. En effet, la localisation permet de déterminer quel régime juridique est applicable. Une localisation au sein de l'Union européenne est la garantie de pouvoir bénéficier des protections permises par le droit de l'Union et le régime général de la protection des données (RGPD). C'est un enjeu de sécurité, mais aussi et surtout de souveraineté numérique.

La commission précise toutefois que la localisation ne peut pas être le seul critère utilisé pour apprécier les standards de sécurité de l'hébergement des données. Il y a des données qui sont hébergées de façon sécurisée en dehors de l'Union européenne, c'est pourquoi la Commission européenne peut par exemple prendre des décisions d'adéquation attestant que le niveau de protection des données dans un pays tiers est au moins équivalent à celui permis par le droit de l'Union. Une telle décision d'adéquation vis-à-vis des États-Unis a par exemple été invalidée par la Cour de justice de l'Union européenne.

C'est d'autant plus problématique que des données peuvent être stockées sur des serveurs et dans des centres de données situés dans l'Union européenne, mais hébergées par des logiciels de *cloud* américains. C'est toute la limite de la stratégie actuelle du Gouvernement et de son label « cloud de confiance », accordé alors que des entreprises utilisent des licences de logiciels américains.

La commission appelle à être vigilante sur ce point et à suivre avec attention l'élaboration de l'arrêté ministériel qui définira le contenu du futur audit de cybersécurité, car la localisation ne peut être le seul critère retenu de sécurisation des données.

Enfin, **sur les modalités d'information aux consommateurs et de présentation du dispositif, les principales dispositions votées par le Sénat demeurent inchangées**, permettant d'ouvrir la voie à la mise en place d'un véritable « Cyberscore ».

La commission a adopté cet article sans modification.

Article 3 (non modifié)

Délai d'entrée en vigueur

Cet article vise à fixer un délai d'entrée en vigueur de la présente proposition de loi au 1er octobre 2023.

La commission a adopté l'article 3 sans modification.

I. Le dispositif initial

Le dispositif initial ne prévoyait pas de délai d'entrée en vigueur de cette proposition de loi.

II. La position du Sénat en première lecture

Lors de l'examen en première lecture au Sénat, aucun délai d'entrée en vigueur de cette proposition de loi n'avait été prévu.

III. Les modifications apportées par l'Assemblée nationale

En séance, l'Assemblée nationale a adopté un amendement du rapporteur introduisant un délai d'entrée en vigueur de cette proposition de loi au 1er octobre 2023.

IV. La position de la commission

Si ce délai semble lointain, la mise en place d'un audit de cybersécurité est inédite et technique. La définition du périmètre d'application et celle du contenu de l'audit de cybersécurité seront respectivement précisées par décret et par arrêté ministériel.

L'élaboration de ces mesures réglementaires nécessite des concertations. La commission considère qu'il est indispensable que les parlementaires, et plus particulièrement les sénateurs, car il s'agit d'une proposition de loi sénatoriale, soient associés à ces consultations afin que l'intention du législateur soit pleinement respectée.

Par ailleurs, la proposition de loi a été notifiée à la Commission européenne à l'issue de son examen en première lecture, conformément aux exigences de la directive européenne de 2015 relative aux services de la société de l'information.

Cette procédure de notification permet à la Commission européenne et aux autres États membres d'examiner, avant leur adoption, les règlements

techniques que les États membres entendent adopter au niveau national concernant les produits et les services de la société de l'information.

Il s'agit de s'assurer que les textes envisagés sont compatibles avec la législation européenne et les principes qui s'appliquent au marché intérieur afin de détecter d'éventuels obstacles à la libre circulation au sein de ce marché.

Cette procédure permet également un dialogue entre les États membres pour identifier les besoins d'harmonisation des législations nationales au niveau de l'Union européenne (UE).

Dans l'éventualité où des observations seront formulées, le Gouvernement devant transmettre de telles informations au Parlement, les consultations liées à l'élaboration des mesures réglementaires d'application pourront permettre de prendre en compte les remarques de la Commission européenne et des autres États membres. La commission sera attentive à ce point.

La commission a adopté cet article sans modification.

EXAMEN EN COMMISSION

Réunie le mercredi 16 février 2022, la commission a examiné le rapport de Mme Anne-Catherine Loisier sur la proposition de loi n° 226 (2021-2022), examinée en deuxième lecture, 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, en deuxième lecture, la proposition de loi de M. Laurent Lafon, président de la commission de la culture, de l'éducation et de la communication du Sénat, pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public.

Mme Anne-Catherine Loisier, rapporteure. – Le dispositif envisagé s'apparente à un « Nutriscore » de la cybersécurité, que nous avons appelé « Cyberscore » et qui doit permettre aux consommateurs usagers d'être mieux informés quant à la protection de leurs données en ligne.

Notre quotidien est de plus en plus virtuel. Nous communiquons par l'intermédiaire de messageries instantanées et, depuis le début de la pandémie, nous travaillons de plus en plus à l'aide de logiciels de visioconférence. Nous nous informons en ligne en consultant les résultats des moteurs de recherche. Nous interagissons sur les réseaux sociaux et nous téléchargeons des applications toujours plus nombreuses pour répondre à nos différents besoins et nous divertir. Mais nous n'avons pas toujours une bonne connaissance des risques qu'entraîne cet usage accru du numérique et une bonne maîtrise des pratiques de sécurité, qui doivent pourtant aller de pair.

Les fuites de données, les piratages des comptes, les escroqueries en ligne, les attaques malveillantes et les failles dans la cybersécurité des entreprises, des hôpitaux, des collectivités territoriales et des administrations sont malheureusement de plus en plus fréquents.

Selon les résultats des récents travaux de la délégation aux entreprises du Sénat sur la cybersécurité des entreprises, en 2020, 43 % des petites et moyennes entreprises (PME) françaises ont constaté un incident de cybersécurité ; 16 % des cyberattaques ont menacé la viabilité même d'une entreprise et les attaques au rançongiciel ont été multipliées par quatre entre 2020 et 2021.

Si tous ces incidents et scandales nous sensibilisent toujours davantage aux enjeux liés à la protection de nos données, nos habitudes de consommation et nos pratiques de production n'évoluent pas comme elles le devraient.

Plusieurs législations nationales et européennes concernent la protection des données, mais les textes en vigueur sont finalement peu orientés vers l'information des consommateurs. C'est cette carence que le présent texte entend combler en créant un dispositif simple, lisible et facilement compréhensible informant les consommateurs du niveau de cybersécurité des solutions numériques qu'ils utilisent.

L'article 1er est relatif au dispositif envisagé, à savoir le Cyberscore.

Le premier enjeu concerne le périmètre d'application.

Alors que la rédaction initiale désignait les opérateurs de plateforme en ligne, nous avions adopté, à l'issue de l'examen en première lecture au Sénat, un périmètre plus large applicable aux fournisseurs de services de communication au public en ligne. Nous avions alors retenu comme cible principale les logiciels de visioconférence, au regard de la généralisation de leur utilisation depuis le début de la crise sanitaire.

Après plusieurs modifications et de nombreuses hésitations du Gouvernement, c'est la notion d'opérateurs de plateforme en ligne qu'a finalement retenue l'Assemblée nationale. Le périmètre a été complété afin d'inclure les systèmes de messagerie instantanée et de visioconférence, conformément à notre souhait initial.

Un décret d'application viendra définir les seuils d'activité au-delà desquels ces acteurs seront concernés. J'insiste, notre cible initiale, c'étaient les plateformes et les services de communication les plus utilisés. À cet égard, la rédaction issue de l'Assemblée nationale satisfait nos attentes.

Le deuxième enjeu à l'article 1er concerne la nature et la dénomination du dispositif.

Au Sénat, nous avions souhaité que ce dispositif ne soit pas trop contraignant ou trop coûteux : il ne faudrait pas qu'il pénalise les très petites entreprises (TPE), les PME ou les start-ups innovantes en matière de services en ligne. À l'Assemblée nationale, la commission des affaires économiques avait adopté un dispositif contraignant de certification par l'Agence nationale de sécurité des systèmes d'information (Anssi). En séance, un équilibre a été trouvé pour que le dispositif de Cyberscore soit, en fait, un « audit de cybersécurité » réalisé par des prestataires agréés de l'Anssi. La notion d'audit se rapproche davantage de ce que nous entendions par diagnostic et permettra des mises à jour régulières. L'équilibre trouvé à l'Assemblée nationale me semble donc également satisfaisant.

Le troisième enjeu à l'article 1er concerne le contenu de cet audit de cybersécurité, qui doit être défini par un arrêté ministériel.

Sous l'impulsion du rapporteur de l'Assemblée nationale et contre l'avis du Gouvernement, nos collègues députés ont adopté un amendement tendant à indiquer que cet audit doit porter sur la sécurisation et la localisation des données. Il s'agit là d'une précision importante, car la

localisation permet de déterminer le régime juridique applicable. Une localisation au sein de l'Union européenne est une meilleure garantie de pouvoir bénéficier des protections permises par le droit communautaire et le règlement général sur la protection des données (RGPD). C'est un enjeu, non seulement de sécurité, mais aussi de souveraineté numérique.

Toutefois, la localisation ne peut pas être le seul critère pour apprécier les standards de sécurité de l'hébergement des données. Certaines données sont hébergées de manière sécurisée en dehors de l'Union européenne. À l'inverse, dans certains pays de l'Union, comme l'Irlande, le degré de protection des données est insatisfaisant.

C'est pourquoi il importe que la Commission européenne puisse prendre des décisions d'adéquation ou de standard attestant que le niveau de protection des données dans un pays tiers est au moins équivalent à celui permis, majoritairement, par le droit de l'Union. Une telle décision d'adéquation à l'égard des États-Unis a par exemple été invalidée par la Cour de justice de l'Union européenne (CJUE) dans l'arrêt *Privacy Shield* de 2020.

On ne saurait l'ignorer : les données peuvent être stockées sur des serveurs et dans des centres de données situés dans l'Union européenne, mais hébergées par des logiciels de *cloud* américains. On touche là les limites de la stratégie actuelle du Gouvernement et de son label « *cloud* de confiance », accordé alors que des entreprises utilisent des licences de logiciels américains. Nous devrons donc être vigilants sur ce point et suivre avec attention l'élaboration de l'arrêté ministériel qui définira le contenu du futur audit de cybersécurité.

Malgré ces réserves, le texte voté par l'Assemblée nationale est acceptable.

Le quatrième et dernier enjeu à l'article 1er concerne les modalités d'information aux consommateurs et de présentation du dispositif.

Au Sénat, nous avions opté pour un dispositif lisible, clair et compréhensible, grâce au système coloriel qui s'inspire de la présentation que nous connaissons avec le Nutriscore. Nos collègues députés ont maintenu ces dispositions.

L'article 2 visait à modifier les règles applicables à la commande publique pour prendre en compte des « impératifs de cybersécurité ». En commission, nous avions émis certaines réserves quant à la validité juridique de ces dispositions, qui ont été supprimées en séance. L'Assemblée nationale n'est pas revenue sur ces suppressions, ce qui permet de centrer le texte sur l'information des consommateurs.

Enfin, un troisième article a été ajouté à l'Assemblée nationale afin de prévoir un délai d'entrée en vigueur, fixé au 1er octobre 2023. Cette échéance peut sembler lointaine, mais la réalisation d'un audit de

cybersécurité est à la fois inédite et très technique. La définition du périmètre d'application nécessitera donc beaucoup de concertations. De ce fait, l'introduction d'un tel délai me semble justifiée.

Les mesures réglementaires d'application sont nombreuses et le Gouvernement nous a indiqué que des consultations seraient menées pour préparer leur élaboration. Nous le lui rappellerons : il est indispensable que les parlementaires, et plus particulièrement les sénateurs, qui ont pris l'initiative de ce texte, soient associés à ces consultations.

Cette proposition de loi a été notifiée à la Commission européenne à l'issue de son examen en première lecture, conformément aux exigences de la directive européenne de 2015 relative aux services de la société de l'information. Dans l'éventualité où des observations seraient formulées, le Gouvernement devra transmettre ces informations au Parlement. Les consultations liées à l'élaboration des mesures réglementaires d'application permettront de prendre en compte les remarques de la Commission européenne et des autres États membres. Nous y serons attentifs.

Ainsi, au-delà de quelques points d'alerte, les modifications votées par l'Assemblée nationale nous semblent aller dans le bon sens. Je vous propose donc un vote conforme.

M. Jean-Pierre Moga. – Je tiens à féliciter notre rapporteure ; les élus de notre groupe voteront ce texte conforme.

EXAMEN DES ARTICLES

Article 1er

L'article 1er est adopté sans modification.

Article 3

L'article 3 est adopté sans modification.

La proposition de loi est adoptée sans modification.

LISTE DES PERSONNES ENTENDUES

Jeudi 10 février 2022

- *Ministère de l'économie, des finances et de la relance, cabinet du secrétaire d'État chargé de la transition numérique et des communications électroniques :* **Mme Carole VACHET**, directrice de cabinet, et **M. Charles-Pierre ASTOLFI**, conseiller Régulations et Communs numériques ;

- *Assemblée nationale :* **M. Christophe NAEGELEN**, député et rapporteur pour la commission des affaires économiques.

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