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

CERTIFICATION DE CYBERSÉCURITÉ DES PLATEFORMES NUMÉRIQUES DESTINÉE AU GRAND PUBLIC

1. 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.

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

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

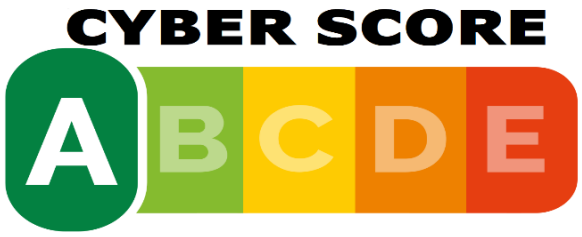
Les consommateurs, quant à eux, sont protégés, en tant que personnes physiques, par le règlement général de protection des données adopté au niveau européen en 2016. Celui-ci n'impose cependant pas d'informer sur le niveau de cybersécurité des solutions proposées par un prestataire de solutions numériques. 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 publics. La cellule « numérique » de suivi de la crise mise en place par la commission des affaires économiques lors du confinement avait d'ailleurs plaidé pour que la Banque des territoires développe une offre d'ingénierie dédiée à l'accompagnement des collectivités en matière de cybersécurité.

2. 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.

POUR EN SAVOIR +

- **Rapport de la délégation aux entreprises du Sénat : « La cybersécurité des entreprises – Prévenir et guérir : quels remèdes contre les cyber virus ? »**
- **Rapport de la délégation aux collectivités territoriales du Sénat : « Les collectivités territoriales face au défi de la cybersécurité »**
- **Baromètre 2022 sur la cybersécurité des entreprises du CESIN**

Sophie Primas
Présidente

Sénateur
des Yvelines
(Les Républicains)

Anne-Catherine Loisier
Rapporteure

Sénatrice
de la Côte-d'Or
(Union Centriste)

COMMISSION
DES AFFAIRES ÉCONOMIQUES
http://www.senat.fr/commission/affaires_economiques/index.html
Téléphone : 01.42.34.23.20
Consulter le dossier législatif :
http://www.senat.fr/dossier-legislatif/ppl19-629.html