N° 4700

———

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 18 novembre 2021.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES AFFAIRES ÉCONOMIQUES

SUR LA PROPOSITION DE LOI, adoptée par le Sénat, *pour la mise en place d'une* **certification** *de* **cybersécurité** *des* **plateformes numériques** *destinée au* **grand public** (n° 3473)

PAR M. CHRISTOPHE NAEGELEN

Député

———

Voir les numéros :

Sénat : **629** (2019-2020)**, 38, 39** et T.A. **008** (2020-2021).

Assemblée nationale : **3473.**

SOMMAIRE

___

Pages

INTRODUCTION 5

I. UN ENVIRONNEMENT NUMÉRIQUE PLUS OUVERT, PLUS COMPLEXE ET PLUS DANGEREUX 7

A. UN ENVIRONNEMENT NUMÉRIQUE PLUS OUVERT ET PLUS COMPLEXE 7

1. Un environnement numérique toujours plus ouvert 7

2. Un environnement numérique toujours plus complexe 7

B. LA CYBERSÉCURITÉ, UN ENJEU LARGEMENT SOUS-ESTIMÉ 8

1. La cybersécurité, un enjeu encore méconnu 8

2. Visioconférences et messageries, une cybersécurité en berne 9

II. L'OBJET DE LA PRÉSENTE PROPOSITION DE LOI : POUR UNE MEILLEURE INFORMATION DES CITOYENS, METTRE EN PLACE UNE CERTIFICATION DE CYBERSÉCURITÉ DES PLATEFORMES NUMÉRIQUES DESTINÉES AU GRAND PUBLIC 10

A. UN CADRE JURIDIQUE COMPLEXE ET ENCORE INSUFFISANT 10

1. Un cadre juridique restreint à la protection des données : le Règlement général sur la protection des données (RGPD) 10

2. Un cadre juridique encore lacunaire concernant la cybersécurité : les avancées timides de l'Union européenne 11

B. MIEUX INFORMER LES CITOYENS : METTRE EN PLACE UNE CERTIFICATION DE CYBERSÉCURITÉ DES PLATEFORMES NUMÉRIQUES DESTINÉES AU GRAND PUBLIC 13

1. Sécuriser les sites les plus utilisés par les consommateurs : simplification et exemplarité 13

2. Inclure les sites de visioconférences et les messageries les plus utilisés 14

3. Création d'un nouveau dispositif de certification intégrant un « cyberscore » 14

4. Rendre facilement identifiable le cyberscore 14

COMMENTAIRE DES ARTICLES 17

Article 1er (art. L. 111-7-3 [nouveau] et L. 131-4 du code de la consommation) : Création d'une certification de cybersécurité des plateformes numériques destinées au grand public 17

Article 2 (Supprimé) : Introduction d'une obligation de respect de la cybersécurité dans la commande publique 19

EXAMEN EN COMMISSION 21

LISTE DES PERSONNES AUDITIONNÉES 29

INTRODUCTION

Menace bien réelle et pourtant invisible pour la plupart des utilisateurs de plateformes numériques, de messageries électroniques et de logiciels de conférences, la cybermalveillance est aujourd'hui insuffisamment prise en compte dans le débat public.

Connaître le niveau de cybersécurité des plateformes que l'on utilise devient non seulement un enjeu citoyen mais également un enjeu individuel, qui consiste à pouvoir protéger ses données personnelles de tout type d'actes de malveillance, délictuels ou criminels.

Le monde virtuel comme le monde réel comportent des menaces, celles du monde virtuel n'en sont pas moins graves du fait des effets induits dans le monde réel (chantage, usurpation d'identité, vol d'argent par la captation des données bancaires, notamment).

La navigation sur internet, notamment sur les plateformes qui accueillent le nombre le plus important d'utilisateurs, offre une fausse impression de sécurité du fait de cette fréquentation élevée. Pourtant les risques liés à la cybermalveillance sont tout aussi élevés voire peut-être davantage que ceux existant sur des plateformes ou messageries plus confidentielles.

Ainsi, en septembre dernier, plus de 700 millions d'utilisateurs de LinkedIn, le plus grand réseau social professionnel, se sont vus dérober leurs données personnelles, divulguées sur internet. En avril, les données de 500 millions d'utilisateurs de ce même réseau social s'étaient retrouvées en vente sur internet, après le piratage massif qui avait précédemment touché les utilisateurs de Facebook, pour ne parler que des événements les plus récents.

Il est temps d'agir pour que les utilisateurs de ces plateformes ne soient ni captifs, ni inconscients des risques qu'ils encourent dans leur usages numériques quotidiens.

La présente proposition de loi a pour origine, un texte déposé en première lecture, au Sénat, par notre collègue sénateur du Val-de-Marne, M. Laurent Lafon.

Le cœur du dispositif, cette proposition de loi propose de rendre obligatoire, pour les plateformes numériques, une certification ainsi que de présenter un diagnostic de cybersécurité, sous la forme d'un diagramme coloré prenant en compte les différents niveaux de sécurité du site pour se protéger des cyberattaques visant la protection des données personnelles hébergées.

Votre rapporteur, après avoir mené des auditions avec les services concernés – direction générale des entreprises (DGE), direction générale de la concurrence et de la répression des fraudes (DGCRF), Agence nationale de la

sécurité des systèmes d'information (ANSSI) – a souhaité enrichir, sous forme d'amendements, votés par la commission, le présent dispositif pour mieux répondre aux attentes des utilisateurs et leur offrir une sécurité plus grande en :

– resserrant le dispositif autour des plateformes qui reçoivent au moins cinq millions de visiteurs uniques par mois ;

– incluant les services de messageries électroniques les plus utilisés ainsi que les services de visioconférence ;

– en introduisant une certification du diagnostic de cybersécurité qui ne pourra plus s'apparenter à un auto-diagnostic mais devra désormais reposer sur une certification faite par l'ANSSI ou par une entreprise que l'ANSSI a habilité à le délivrer ;

– en étendant le diagnostic de sécurisation non plus aux seules données personnelles mais également à la sécurisation des sites internet eux-mêmes ;

Parce que la cybersécurité demeure un enjeu crucial pour pouvoir naviguer sur les plateformes numériques, ou dialoguer par messagerie ou visioconférence, en toute sécurité, la présente proposition de loi, enrichie par les travaux de la commission, pose la première pierre de l'édifice, la première pierre de ce mur de la cybersécurité qu'il reste à construire pour restaurer la confiance dans nos liaisons numériques.

I. UN ENVIRONNEMENT NUMÉRIQUE PLUS OUVERT, PLUS COMPLEXE ET PLUS DANGEREUX

A. UN ENVIRONNEMENT NUMÉRIQUE PLUS OUVERT ET PLUS COMPLEXE

1. Un environnement numérique toujours plus ouvert

La crise sanitaire liée à l'épidémie de Covid-19 **a mis en lumière notre interdépendance numérique**. Alors que nos concitoyens étaient privés en partie de leur liberté d'aller et venir, le déploiement de l'environnement numérique s'est considérablement étendu à la faveur de la crise, accentuant une tendance déjà largement présente dans tous les secteurs d'activité.

Ce déploiement numérique, une fois le retour à la « vie normale » intervenu, continue son expansion, **soulevant dès lors d'autant plus la question de la sécurité des données – et, plus précisément, celle des données personnelles présentes et hébergées sur les sites internet – que nos interactions numériques sont quotidiennes**.

Ce phénomène est d'autant plus prégnant que le **Gouvernement ambitionne de dématérialiser 100 % des 250 démarches les plus utilisées par les citoyens d'ici mai 2022**. De volontaire, la démarche numérique deviendra contrainte pour un certain nombre de démarches, accentuant pour certains la fracture numérique, **mais surtout la nécessité d'interagir dans un environnement sécurisé.**

Si les sites gouvernementaux présentent un niveau de sécurité élevé face aux cyberattaques, qu'en-est-il exactement des sites les plus utilisés par les consommateurs – plateformes de vente en ligne, banques en ligne, sites de commerce en ligne ?

Pourtant sensibles aux questions de sécurité en elles-mêmes, les consommateurs ignorent souvent tout de la complexité de l'environnement numérique et de la sécurité des sites qu'ils utilisent ou qui hébergent leurs données, les soumettant de fait à une fragilité qui n'est pas sans danger.

2. Un environnement numérique toujours plus complexe

Chaque fois qu'un consommateur effectue une opération en ligne, clique sur un site, navigue sur internet ou échange des messages sur des messageries grand public (*Messenger* ou *Whatsapp*, pour ne citer que les plus connues d'entre elles) – et d'autant plus que ses interactions numériques lui sont devenues familières du fait d'un usage régulier, voire quotidien –, il semble oublier que ses données personnelles peuvent être constamment piratées, qu'il peut faire l'objet d'un chantage numérique, que son identité peut être usurpée et que ses comptes en banque peuvent être vidés à distance, du fait de la cybermalveillance.

Cette ignorance tient en grande partie **à la complexité de l'environnement numérique ainsi qu'à la dématérialisation des données**. Un site sur lequel se connecte un consommateur peut parfaitement être vulnérable alors, qu'*a priori*, la surface publicitaire ou le poids financier de celui qui l'édite semblerait garantir le consommateur de toutes formes d'attaques.

En effet, la complexité de l'environnement numérique repose notamment sur une forte dématérialisation des données. Ainsi, un site hébergé en France peut parfaitement stocker les données personnelles de ses utilisateurs **dans un pays tiers, dans lequel la législation française ou européenne, relativement protectrice, ne s'appliquera pas.** Ce pays tiers pourra ensuite revendre ces données ou les utiliser à des fins autres que commerciales, comme des fins d'espionnage ou de chantage, ainsi que l'on rappelé à juste titre la direction générale des entreprises (DGE) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

En outre, **l'agilité de la cyberdélinquance se développe de concert avec l'ouverture de l'environnement numérique** et sa virtualité ne la rend pas moins dangereuse ou criminelle**. La complexité de l'architecture des sites internet peut également masquer autant de failles de sécurité** que ceux-ci proposent de services diversifiés à leurs clients.

Exiger de la part des plateformes les plus utilisées par les consommateurs une certification en termes de cybersécurité semble, dès lors, pour votre rapporteur, un préalable : préalable pour mieux informer le consommateur des risques qu'il encourt ; préalable en termes d'exemplarité pour l'ensemble de sites fournissant des services de communication au public en ligne ; préalable, enfin, à une harmonisation de la législation européenne à un haut niveau de sécurité.

B. LA CYBERSÉCURITÉ, UN ENJEU LARGEMENT SOUS-ESTIMÉ

1. La cybersécurité, un enjeu encore méconnu

Par cybersécurité, on entendra **l'ensemble des dispositifs techniques permettant de préserver la disponibilité, l'intégrité et la confidentialité des données et des services numériques.**

Enjeu encore trop largement méconnu du grand public, **la cybersécurité ne doit pas rester une question de spécialistes et doit être abordée dans le débat public**. En effet, **la cyberdélinquance est la délinquance de demain**, dont tous les effets n'ont pas encore été entièrement mesurés.

Qu'il s'agisse de **rançongiciels** – c'est-à-dire l'utilisation de logiciels permettant de bloquer l'accès à un site en échange d'une rançon –, de vols de données personnelles ou d'usurpation d'identité, la cyberdélinquance se développe à l'aune de la numérisation de notre environnement quotidien.

En outre, la possibilité non seulement d'enregistrer des données personnelles, mais également de créer de faux contenus à l'insu de la personne utilisatrice d'une plateforme, demeure un risque dont l'ampleur n'a pas encore entièrement été évaluée.

Plus l'environnement numérique demeure ouvert, plus l'enjeu en termes de cybersécurité devient important.

Sont particulièrement exposés à la cybermalveillance, outre **les plateformes recevant plus de cinq millions de visiteurs par mois, les outils plébiscités par les consommateurs que sont les messageries en ligne grand public et les outils de visioconférence.**

2. Visioconférences et messageries, une cybersécurité en berne

La récente crise sanitaire a montré tant la méconnaissance générale de l'ensemble de la population, qui a recours aux nombreux services en ligne sans se préoccuper des enjeux de sécurité, que l'impréparation relative de l'État **concernant les logiciels de conférence en ligne ou de messagerie sécurisée, dont le marché est très largement dominé par des produits d'origine américaine** (*Zoom, Lifesize* ou *Whatsapp*, pour ne citer que les plus connus d'entre eux).

Très présents sur le marché, accessibles, connus, ces logiciels de conférences en ligne ou de messagerie sécurisée ont été largement utilisés par les consommateurs lors de la crise sanitaire et continuent à l'être, notamment par nombre d'entreprises pour leurs conférences internes et stratégiques, certains services de l'État ou par des établissements d'enseignement supérieur pour la dispense de cours.

Si certains services de l'État, comme ceux liés à la défense et aux affaires étrangères, notamment, ont clairement interdit à leurs agents d'utiliser les services de certaines conférences en ligne pour défaut de sécurité des informations échangées, **le recours à *Zoom* ou *Lifesize* a néanmoins été massif lors de la dernière crise sanitaire.**

L'utilisation de la messagerie ***Tchap*** [(1)], messagerie sécurisée et développée par le Gouvernement, est ainsi restée marginale **alors qu'elle offre une sécurité réelle en termes d'échange du fait du cryptage des données de bout en bout de la conversation et de l'obligation d'autoriser l'échange par une clé d'authentification connue des seuls participants à celui-ci**. Son insuccès relatif s'explique par une double limite, à savoir une notoriété moindre et un accès moins facile et moins intuitif par comparaison avec d'autres messageries comme *Whatsapp*, par exemple.

Il en est de même **du logiciel de conférence *TIXEO***, seul éditeur de visioconférence à ce jour à avoir reçu le visa de sécurité ANSSI 2021.

---

(1) https://www.numerique.gouv.fr/outils-agents/tchap-messagerie-instantanee-État/

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a pour mission de garantir la sécurité et la défense des systèmes d'information de l'ÉTAT et des sociétés classées comme opérateurs d'importance vitale (OIV). Le **niveau de certification qu'elle délivre** correspond à des standards particulièrement élevés.

Evaluer la sécurité des plateformes qui reçoivent le plus d'utilisateurs, des messageries les plus utilisées ainsi que des outils de conférence en ligne représente **pour votre rapporteur un enjeu citoyen de la plus haute importance**. C'est la raison pour laquelle la présente proposition de loi a notamment pour objet de proposer **un « cyberscore »**, sur le modèle du « nutriscore » ou du diagnostic énergétique, et qui permettrait, en fonction du niveau de certification délivré, **de mesurer les risques pris au quotidien dans nos usages et liaisons numériques.**

II. L'OBJET DE LA PRÉSENTE PROPOSITION DE LOI : POUR UNE MEILLEURE INFORMATION DES CITOYENS, METTRE EN PLACE UNE CERTIFICATION DE CYBERSÉCURITÉ DES PLATEFORMES NUMÉRIQUES DESTINÉES AU GRAND PUBLIC

A. UN CADRE JURIDIQUE COMPLEXE ET ENCORE INSUFFISANT

La présente proposition de loi, issue d'une proposition de notre collègue sénateur Laurent Lafon, a été substantiellement modifiée lors des débats au Palais du Luxembourg.

Alors l'article 2 de la proposition de loi, qui avait pour objet de faire respecter l'objectif de cybersécurité dans la commande publique, insuffisamment sécurisé sur le plan juridique, a été supprimé, **l'article 1er** a **été, en quelque sorte, vidé de sa substance initiale** par le jeu des modifications qui y ont été apportées.

Examinée en première lecture devant notre assemblée, cette proposition de loi mérite d'être rendue à son ambition initiale, au regard de l'enjeu citoyen qu'elle représente.

Les auditions conduites par votre rapporteur l'amènent ainsi à proposer une série d'amendements, pour revenir à l'esprit de l'initiative de notre collègue sénateur **mais également pour l'enrichir, pour en sécuriser le dispositif juridique, afin de mieux prendre en compte les enjeux de cybersécurité**, au cœur de la nécessité de promouvoir une **meilleure information des consommateurs à travers un nouvel outil, celui d'une certification qui pourrait s'apparenter à un cyberscore.**

1. Un cadre juridique restreint à la protection des données : le Règlement général sur la protection des données (RGPD)

L'initiative de cette proposition de loi s'enracine dans la volonté d'élargir la protection apportée par le Règlement (UE) 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 (règlement général sur la protection des données), dit **« RGPD », aux données personnelles et à la sécurisation de certaines plateformes recevant plus de cinq millions de visiteurs par mois, des messageries en ligne grand public et des outils de visioconférence.**

Si le RGPD sécurise les données personnelles des consommateurs qui consultent les sites internet, il ne les protège pas, en effet, des failles en termes de cybersécurité, ni n'empêche le transfert des données personnelles collectées par les messageries et les outils de visioconférence.

Le dispositif issu du RGPD peut même donner l'impression fallacieuse que les données personnelles sont entièrement sécurisées, dans la mesure où l'on n'accepterait pas certains « *cookies* » publicitaires, ce qui n'est aucunement le cas, car l'objet de la protection n'est pas identique.

La protection relative à la cybersécurité – exceptée la sécurité et la défense des systèmes d'information de l'État et des sociétés classées comme opérateurs d'importance vitale (OIV), relevant de la mission de l'ANSSI – n'est pas encore garantie pour l'ensemble des sites, loin s'en faut : **tel est le constat qui sous-tend l'idée de proposer un cyberscore** et celle de certifier les plateformes les plus utilisées ainsi que les outils de messagerie et de visioconférence.

2. Un cadre juridique encore lacunaire concernant la cybersécurité : les avancées timides de l'Union européenne

La nécessité d'harmoniser les législations sur une question qui dépasse le cadre national a conduit l'Union européenne à s'emparer du sujet sans que, jusqu'ici, le niveau de protection en termes de cybersécurité **ait encore conduit à une protection de niveau équivalent à celle apportée par le RGPD pour les données personnelles.**

Le **Cybersecurity Act,** règlement européen adopté en 2019 par le Parlement européen et le Conseil, affiche un double objectif :

– adopter le mandat de l'ENISA (*European Union Agency for Cybersecurity)* en renforçant son rôle de soutien à la coopération entre les États membres ;

– définir un cadre commun pour la **certification** de cybersécurité, visant à harmoniser à l'échelle européenne les méthodes d'évaluation et les niveaux d'assurance de la certification. Les certificats délivrés bénéficieront d'une reconnaissance mutuelle au sein de l'Union européenne.

Sont ainsi prévus trois niveaux d'assurance de la certification :

– un niveau élémentaire pour les produits destinés au grand public, considérés non critiques et reposant sur une auto-évaluation ;

– un niveau substantiel ou médian, qui repose sur des tests de conformités effectués par un tiers de confiance accrédité ;

– un niveau élevé pour les produits ou services les plus sensibles (par exemple, des objets médicaux connectés ou des puces pour cartes d'identité), qui nécessite la mise en place de tests très approfondis.

La directive n° 2016/1148, dite directive « NIS », a instauré des obligations harmonisées en matière de sécurité numérique pour les places de marché en ligne, les moteurs de recherche et les services d'informatique en nuage.

Ces obligations sont précisées dans le règlement d'exécution 2018/151 du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil qui précise les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif. Ce règlement indique :

– les éléments à prendre en compte par les fournisseurs de service numérique lorsqu'ils définissent et prennent des mesures visant à assurer un niveau de sécurité des réseaux et des systèmes d'information qu'ils utilisent pour proposer les services ;

– les paramètres pertinents pour déterminer si un incident a un impact significatif sur la fourniture de ces services, incidents déclenchant une obligation de déclaration à l'autorité ou à l'équipe de réponse à incident de l'État membre.

Les modalités de contrôle du respect de ces obligations ont été définies par la 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 (articles 10 à 15), qui a confié à l'ANSSI des pouvoirs de contrôle et de sanction dans les cas de non-conformité prévus par la directive et son règlement d'exécution.

La future présidence française de l'Union européenne, qui prendra effet à compter du 14 janvier 2022, a pour objectif de faire aboutir la négociation en cours entre le Conseil et le Parlement européen et visant, sur la base d'une proposition de directive de la Commission européenne datant de décembre 2020, à étendre le champ d'application de la directive aujourd'hui en vigueur.

Les amendements proposés par votre rapporteur à la présente proposition de loi s'inscrivent dans cet objectif, celui de définir un cadre simple et vertueux pour inciter, à terme, l'ensemble des entreprises à sécuriser leurs sites et informer les consommateurs qui les utilisent.

B. MIEUX INFORMER LES CITOYENS : METTRE EN PLACE UNE CERTIFICATION DE CYBERSÉCURITÉ DES PLATEFORMES NUMÉRIQUES DESTINÉES AU GRAND PUBLIC

1. Sécuriser les sites les plus utilisés par les consommateurs : simplification et exemplarité

Le premier amendement de votre rapporteur réécrit ainsi, en partie, l'article 1er de la proposition de loi prévoyant d'insérer un article additionnel dans le code de la consommation.

L'article 1er de la proposition de loi, dans sa rédaction initiale, visait un triple objectif :

– définir le champ d'application des dispositions concernées ;

– proposer un diagnostic de cybersécurité sous la forme d'un cyberscore, en renvoyant la définition des critères pertinents au pouvoir réglementaire ;

– prévoir de présenter immédiatement ce cyberscore à l'utilisateur dès lors que l'utilisation du service de communication nécessite de s'identifier électroniquement sur le site.

L'amendement présenté par votre rapporteur vise, tout d'abord, à restreindre le champ d'application de la loi, c'est-à-dire les plateformes concernées par une certification de cybersécurité, dans un souci de simplification et d'exemplarité.

Les auditions qu'ils a réalisées ont en effet montré les difficultés, pour des petites plateformes, à effectuer un tel diagnostic. Limiter les nouvelles obligations aux seuls d'opérateurs de taille significative répondra de manière appropriée au double objectif d'efficacité et d'exemplarité.

L'article L. 111-7-1 du code de la consommation renvoie, en effet, à l'article D. 111-15 du même code qui précise que les opérateurs concernés par les obligations de l'article L. 111-7-1 sont ceux **dont le seuil minimal d'activité est fixé à cinq millions de visiteurs uniques par mois.**

Ce seuil concerne donc les plateformes, ainsi que les entreprises, les plus importantes (de l'ordre d'une centaine). Il permet de donner davantage de temps aux entreprises moyennes et aux *start-ups* pour se mettre en conformité avec le droit. Il convient en effet de tenir compte du fait que l'obtention d'une certification de cybersécurité aura un coût, qui peut être conséquent.

Le resserrement du périmètre d'intervention mentionné à l'article L. 111-7-1 précité **correspond à une demande du Gouvernement**, qui n'avait pas été entendue lors des travaux en première lecture devant le Sénat.

L'amendement de votre rapporteur vise également **à limiter le champ d'application du cyberscore à la sécurisation des données hébergées ainsi qu'à la capacité des sites utilisés de se protéger face à des cyberattaques**.

2. Inclure les sites de visioconférences et les messageries les plus utilisés

L'amendement de votre rapporteur vise aussi à **étendre le champ des plateformes concernées par une certification de cybersécurité aux services de visioconférence éligibles au cyberscore,** tout en définissant un seuil d'activité par décret afin de ne viser que les services de visioconférence les plus utilisés (notamment *Zoom, Lifesize, Whatsapp*, etc.).

Les messageries, dans la mesure où elles peuvent également comprendre des failles de sécurité, sont également incluses dans le champ de la proposition de loi, telle que votre rapporteur vous propose de l'amender.

3. Création d'un nouveau dispositif de certification intégrant un « cyberscore »

Le second amendement de fond de votre rapporteur vise à renforcer le dispositif prévu par le Sénat. Tel qu'il est aujourd'hui envisagé, le diagnostic de certification repose sur une auto-déclaration. Il s'agit donc d'un niveau de sécurité faible, voire trompeur pour le consommateur qui pourrait croire à une véritable sécurisation du site concerné.

Le dispositif désormais proposé ne reposerait plus sur une simple auto-déclaration, mais bien sur une certification délivrée directement **par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou par une entreprise habilitée à délivrer une telle certification.**

La proposition de loi **crée un nouveau label, le « cyberscore »**, renvoyant au pouvoir réglementaire le soin d'établir les critères à mettre en œuvre pour le définir. Hormis un amendement de cohérence, visant à remplacer le terme de « diagnostic » par celui de « certification », votre rapporteur a conservé la rédaction initiale de ce texte (article L.111-7-3 [nouveau] du code de la consommation).

Les auditions ont montré que plusieurs critères pourraient être pris en compte, dont celui de garantir, par exemple, que les données ne sont pas exposées à des législations étrangères à portée extraterritoriale, qui autoriseraient l'utilisation de ces données à des fins d'espionnage des usagers.

4. Rendre facilement identifiable le cyberscore

Votre rapporteur conserve l'idée initiale **d'un code couleur pour identifier les niveaux de sécurité assurés par les plateformes et les outils de communication concernés.**

Votre rapporteur a néanmoins souhaité préciser par amendement que la certification devait être bien visible pour le consommateur. Outre sa lisibilité, c'est l'un des premiers éléments qu'il devra voir lorsqu'il se connectera à un site afin de s'assurer de sa fiabilité et de savoir s'il peut continuer à l'utiliser de manière sécurisée.

*

* *

Outre la protection des consommateurs et celle des citoyens, la présente proposition de loi ambitionne de poser **les fondements juridiques d'une meilleure garantie en termes de cybersécurité des plateformes** recevant au moins cinq millions de visiteurs, ainsi que des outils de messagerie électronique et de visioconférence en ligne.

Le dispositif proposé peut également présenter des vertus d'exemplarité dans le cadre de l'Union européenne, à l'heure des débats sur la directive « NIS », de sorte qu'en termes de protection des libertés individuelles, le mieux-disant l'emporte sur la tentation du moins-disant.

Le choix de cibler certains services uniquement est **celui de la sagesse, pour permettre un contrôle efficace et efficient par les services de l'État ainsi qu'une certification de haut niveau.** Votre rapporteur ne doute pas, qu'une fois adopté, **ce niveau de standard élevé finira par s'imposer à l'ensemble des fournisseurs de services de communication au public**.

COMMENTAIRE DES ARTICLES

Article 1er

(art. L. 111-7-3 [*nouveau*] et L. 131-4 du code de la consommation)

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

Article modifié par la commission.

L'article 1er de la présente proposition de loi vise à instituer une certification des plateformes numériques, des services de messagerie et des logiciels de visioconférence à destination du grand public.

I. LES DISPOSITIONS DE L'ARTICLE

Adopté en première lecture au Sénat, l'article 1er modifie le code de la consommation en introduisant un article L. 111-7-3 [*nouveau*] qui a pour objet, de rendre obligatoire, pour certaines plateformes, dont l'activité dépasse un ou plusieurs seuils définis par décret, l'affichage d'un **diagnostic de cybersécurité** portant sur la sécurisation des données qu'ils hébergent, directement ou par l'intermédiaire d'un tiers.

Les critères, pour le diagnostic, sont établis par décret, après avis de la Commission nationale de l'informatique et des libertés, après un arrêté conjoint des ministres chargés du numérique et de la consommation.

Le diagnostic est présenté au consommateur de manière lisible, sous la forme d'un système d'information coloriel, dès que celui-ci s'identifie électroniquement.

II. TRAVAUX DE LA COMMISSION

La commission a **substantiellement modifié**, par voie d'amendements, cet article 1er adopté par le Sénat en première lecture.

Le **premier amendement** vise à restreindre le champ des plateformes concernées par une certification de cybersécurité, dans un souci de simplification et d'exemplarité.

En introduisant une référence à l'article L. 111-7-1, le texte renvoie en effet à l'article D. 111-15 du même code, qui précise que les opérateurs concernés par les obligations de l'art. L. 111-7-1 **sont ceux dont le seuil minimal d'activité est fixé à cinq millions de visiteurs uniques par mois.**

Une centaine d'entreprises sont ainsi concernées par la nouvelle rédaction proposée par un amendement de votre rapporteur.

Il s'agit également de donner davantage de temps aux entreprises de taille moyenne et aux start-ups pour se mettre en conformité avec le droit dans la mesure où l'obtention d'une certification de cybersécurité aura un coût, souhait formulé par le Gouvernement, en première lecture, au Sénat, mais qui n'avait pas été entendu.

Cet amendement étend également le champ de l'obligation d'une certification de cybersécurité aux services de visioconférence ainsi qu'aux messageries les plus utilisées tout en définissant leur seuil d'activité par décret afin de ne viser que les plus utilisés d'entre eux tels, notamment, Zoom, Lifesize, Whatsapp, Messenger,…

Cet amendement vise aussi à faire entrer dans le domaine de la sécurité des plateformes, les sites eux-mêmes et pas seulement la sécurité des données personnelles.

Le second amendement présenté par votre rapporteur propose de lever les ambiguïtés de la précédente rédaction qui auraient pu induire les consommateurs en erreur en laissant croire à une véritable sécurisation des sites alors que le diagnostic de cybersécurité aurait reposé sur simple auto-déclaration.

Votre rapporteur a donc proposé de remplacer le terme de diagnostic de cybersécurité par celui de **certification**, certification qui sera effectuée soit directement par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) soit par les entreprises qu'elle a habilitées à le faire.

Votre commission a également adopté des amendements rédactionnels de cohérence pour remplacer le terme de « diagnostic » par celui de « certification ». La commission a adopté l'article 1er ainsi modifié.

*

* *

Article 2
(Supprimé)

Introduction d'une obligation de respect de la cybersécurité dans la commande publique

Maintien de la suppression par la commission.

I. L'ÉTAT DU DROIT

Supprimé en première lecture au Sénat, pour défaut de sécurisation juridique, votre rapporteur n'a pas souhaité déposer d'amendement pour rétablir l'article 2, au regard de ce défaut de sécurisation juridique, préférant poser les jalons du droit de la cybersécurité avec l'article 1er.

II. TRAVAUX DE LA COMMISSION

Aucun amendement n'a été déposé pour rétablir l'article 2 devant la Commission. Votre commission a maintenu la suppression de l'article 2.

EXAMEN EN COMMISSION

Au cours de sa séance du jeudi 18 novembre 2021, la commission des affaires économiques a ensuite examiné la proposition de loi, adoptée par le Sénat, pour la mise en place d'une certification de cybersécurité des plateformes numériques destinées au grand public (n° 3473), sur le rapport de M. Christophe Naegelen.

M. Christophe Naegelen, rapporteur. Cette proposition de loi vise à apporter une réponse efficace et novatrice à la menace insuffisamment évaluée et quantifiée qu'est la cyberdélinquance. La cybersécurité ne peut pas rester une question de spécialistes ; le grand public doit s'en saisir, car notre environnement numérique est désormais ouvert, complexe et dangereux. À chacun de vos clics, vous risquez de perdre vos données personnelles, d'être victimes, d'une usurpation de votre identité ou d'un rançongiciel. Qui, parmi nous, est réellement conscient de ces dangers ? Il est temps d'agir !

Déposée par notre collègue sénateur Laurent Lafon, la présente proposition de loi est ressortie des débats au Sénat avec son article 1er substantiellement modifié et son article 2 supprimé. Il nous revient de lui rendre son ambition initiale, mais aussi de l'enrichir. À cet effet, je vous proposerai des amendements issus des travaux que nous avons conduits, Mme Huguette Tiegna et moi-même. Ils ont vocation à sécuriser le dispositif juridique et à promouvoir une meilleure information des consommateurs à travers un nouvel outil, celui d'une certification qui pourrait s'apparenter à un cyberscore.

Ces amendements ont été élaborés en concertation avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui a pour mission de garantir la sécurité et la défense des systèmes d'information de l'État et des sociétés classées opérateurs d'importance vitale (OIV), avec la direction générale des entreprises, la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), les représentants des entreprises et le ministère chargé du numérique. Ils ont pour but d'obliger les sites les plus importants à obtenir une certification d'absence de vulnérabilité aux cyberattaques. Afficher un cyberscore sera la preuve que l'on a obtenu une certification et que la navigation est sécurisée.

Les auditions ayant mis en évidence les difficultés à effectuer un diagnostic pour de petites plateformes, dans un souci de simplification et d'exemplarité, seront sécurisés les sites les plus utilisés par les consommateurs. Un premier amendement tendra à réécrire en partie l'article 1er en insérant un article additionnel dans le code de la consommation.

Les sites visés sont ceux dont le seuil minimal d'activité est fixé à 5 millions de visiteurs uniques par mois, ce qui concerne une centaine de plateformes et d'entreprises. Ce seuil permet de donner davantage de temps aux entreprises moyennes et aux start-up pour se mettre en conformité avec le droit. Il convient en effet de tenir compte du fait que l'obtention d'une certification de cybersécurité a un coût, qui peut être important.

L'amendement vise également à limiter le champ d'application du cyberscore à la seule sécurisation des données hébergées ainsi qu'à la capacité des sites utilisés de se protéger face à des cyberattaques.

Il étend le champ des plateformes concernées par la certification aux services de visioconférence, renvoyant à un décret la fixation du seuil d'activité afin de ne viser que les plus utilisés – Zoom, Lifesize, WhatsApp –, mais aussi aux messageries les plus importantes, comme Messenger ou WhatsApp, qui peuvent également présenter des failles de sécurité. J'en profite pour rappeler qu'il existe des outils sécurisés, encore trop méconnus, comme le logiciel TIXEO, certifié par l'ANSSI pour les visioconférences, ou le service de messagerie Tchap, crypté de bout en bout.

Les auditions ont montré que plusieurs critères pourraient être pris en compte, dont celui visant à garantir, par exemple, que les données ne sont pas exposées à des législations étrangères à portée extraterritoriale, qui autoriseraient l'utilisation de ces données à des fins d'espionnage des usagers.

Mon second amendement vise à renforcer le dispositif prévu par le Sénat, qui fait reposer le diagnostic de certification sur une déclaration. Le niveau de sécurité est donc très faible, voire trompeur pour le consommateur. C'est comme si, à l'école, on demandait à un élève de corriger lui-même sa dictée ! Avec ma proposition, la certification sera délivrée directement par l'ANSSI ou par une entreprise qu'elle aura habilitée.

J'ai tenu à conserver l'idée initiale d'un code couleur pour identifier les niveaux de sécurité assurés par les plateformes et les outils de communication. J'ai cependant déposé un amendement pour que cette certification soit visible dès la connexion, afin que l'internaute puisse décider sciemment de poursuivre ou non sa navigation.

En posant les fondements juridiques d'une garantie de cybersécurité pour les plateformes les plus visitées, cette proposition de loi ambitionne également de devenir un exemple au sein de l'Union européenne, à l'heure où est discutée la directive dite Network and information system security ou NIS, de sorte qu'en matière de protection des libertés individuelles, le mieux-disant l'emporte sur la tentation du moins-disant. Le choix de cibler uniquement certains services est celui de la sagesse, afin de permettre un contrôle efficace et efficient par les services de l'État, ainsi qu'une certification de haut niveau. Je ne doute pas qu'une fois adopté, ce niveau de standard élevé finira par s'imposer à l'ensemble des fournisseurs de services de communication au public. C'est pourquoi je vous demande de voter cette proposition de loi novatrice, en lui donnant une valeur d'exemple.

Mme Huguette Tiegna (LaREM). La crise sanitaire liée à l'épidémie de la covid-19 a mis en lumière notre interdépendance numérique. Nos concitoyens, privés de leur liberté de mouvement, se sont massivement tournés vers le monde digital, aussi bien dans le domaine des loisirs que dans tous les secteurs d'activité – click and collect, passe numérique, visite de musées en ligne, télétravail…

Les restrictions sanitaires une fois levées, le numérique a continué de croître, soulevant encore davantage la question de la sécurité des données et, plus précisément, celle des données personnelles présentes et hébergées sur les sites internet. Les fuites de données personnelles représentent une des principales menaces de cybersécurité.

L'encadrement de la protection des données personnelles a été renforcé, tant au niveau européen par l'adoption du règlement général sur la protection des données personnelles (RGPD) en 2016, qu'au niveau national avec la loi du 20 juin 2018 relative à la protection des données personnelles. La présente proposition de loi s'engage dans la même voie, en cherchant toutefois à sécuriser les données personnelles numériques beaucoup plus efficacement. La récente audition par la commission des affaires économiques et de la commission des lois de Mme Frances Haugen, ancienne cadre de Facebook et lanceuse d'alerte, nous a confirmé que le modèle économique de Facebook s'appuie sur l'extraction et l'analyse des données personnelles, dans des proportions gigantesques, notamment pour la publicité ciblée. La cybersécurité est bien trop souvent sous-estimée. C'est un enjeu méconnu du grand public, qui doit être abordé dans le débat public. D'après l'ANSSI, le nombre de cyberattaques a été multiplié par quatre en 2020.

Le groupe LaREM soutiendra la proposition de loi, qui vise à mettre en œuvre des pratiques plus vertueuses en permettant aux utilisateurs de bénéficier d'une information claire et compréhensible sur les conditions d'hébergement de leurs données personnelles, de leur assujettissement à des lois extraterritoriales et de leur exploitation à des fins commerciales. M. le rapporteur a raison, la certification doit être plus rigoureuse.

M. Philippe Latombe (Dem). Le groupe Mouvement démocrate et démocrates apparentés soutiendra la proposition de loi. La mission d'information de la Conférence des présidents sur la souveraineté numérique française et européenne, dont j'étais le rapporteur, a mis en lumière l'importance de la cybersécurité pour les acteurs économiques, les collectivités territoriales, mais aussi les consommateurs. L'Europe a fait de gros efforts en matière de protection des données personnelles et le RGPD a fait son chemin dans la société et auprès des consommateurs.

Il faut désormais aller plus loin – c'était également l'une des conclusions du rapport à la suite des auditions. Il faut que les consommateurs soient conscients de ce qu'est la cybersécurité et des moyens dont ils disposent dans le monde numérique pour être protégés. La proposition de loi participera à l'éducation de tous les acteurs de la société. En introduisant la transparence à laquelle a appelé Mme Frances Haugen lors de son audition, la rédaction que vous proposerez permettra aux consommateurs de reprendre la main.

C'est aussi pour cette raison que nous avons déposé un amendement sur la localisation des données, élément majeur de sécurisation pour le consommateur dans le cadre du RGPD, surtout depuis la décision de la Cour de justice de l'Union européenne d'invalider le privacy shield. Peut-être ne serons-nous pas d'accord avec le rapporteur – mais je ne préjuge pas de sa décision. Mme Frances Haugen l'a rappelé, une fois que Facebook a des données, on ne sait plus où elles sont stockées ni comment elles sont

traitées. Pourtant, c'est extrêmement important pour les consommateurs et tous les acteurs du numérique.

M. Philippe Naillet (SOC). Ce texte apporte une utile contribution au renforcement de la protection des données de nos concitoyens, dans un contexte de développement accéléré des usages numériques. On ne compte plus les articles de presse relatant des fuites de mots de passe, voire de données personnelles importantes, subies par des sites et plateformes offrant des services de communication au public, émanant parfois de sociétés dont l'assise inspire pourtant confiance. Parfois, ces fuites de données ont des conséquences graves pour nos concitoyens lorsqu'elles donnent lieu à des usurpations d'identité ou à l'utilisation frauduleuse d'outils bancaires. Ces difficultés concernent également les entreprises qui utilisent ces outils numériques, qui peuvent être victimes d'espionnage industriel ou de malveillances affectant leur valeur et leurs résultats.

La société attend, et c'est notre responsabilité de parlementaires de répondre à cette attente, que ces plateformes soient contraintes d'assurer un niveau de cybersécurité à même de protéger autant que possible les données privées. L'article 1er de la proposition de loi prévoit une présentation lisible et compréhensible, par le biais d'un système d'affichage de type nutri-score, qui satisfait l'ambition de bonne information du public. Bien entendu, en renvoyant au pouvoir réglementaire la définition des critères pris en compte dans l'évaluation, le texte laisse à ce dernier une large marge d'appréciation. Nous souhaitons que ces critères soient extensifs et ambitieux, au risque sinon de priver d'objet la disposition. L'ANSSI devra jouer pleinement son rôle dans ce processus, alors que l'État ne brille habituellement pas en matière de sécurité numérique.

Nous sommes également favorables aux dispositions prévues à l'article 2 qui prévoient de renforcer la prise en compte des impératifs de cybersécurité dans les marchés publics, et en particulier dans la définition précise du besoin. Considérant la sensibilité de certaines des données recueillies et utilisées par les collectivités locales, comme par les administrations de l'État, il s'agit d'une bonne mesure mais elle impliquera un accompagnement des petits acheteurs publics qui ne disposent pas nécessairement des moyens d'ingénierie pour intégrer pleinement cette dimension dans leur politique d'achat. L'Agence nationale de la cohésion des territoires (ANCT) pourrait utilement apporter son concours en complément des mutualisations existantes entre collectivités en matière d'information et de systèmes d'information.

Enfin, comme le Sénat, nous regrettons que ce texte ne s'adresse pas directement aux entreprises qui sont soumises aux mêmes risques s'agissant de la protection de leurs données. Cependant, et considérant les évolutions positives de la proposition de loi en matière de scoring et d'information du public, nous voterons pour.

M. Thierry Benoit (UDI-I). Le groupe UDI et indépendants soutiendra la proposition de loi de notre collègue Christophe Naegelen, dans le droit fil de ses précédentes initiatives. Ce texte, bien de notre temps, vise à certifier la performance de sécurité des plateformes numériques en luttant contre toute forme de piratage, afin de protéger les usagers et les consommateurs de services numériques.

J'espère que notre vote sera unanime, afin que la France soit un modèle au sein de l'Union européenne, à l'heure où son Président va en prendre la présidence. Cette proposition de loi, comme avant elle celle de Mme Patricia Lemoine, illustre bien le rôle des parlementaires qui se doivent de coller à la réalité de ce que vivent nos concitoyens.

M. Antoine Herth (Agir ens). Nous accueillons favorablement cette proposition de loi. Pour les entreprises, le numérique crée autant d'opportunités économiques que, malheureusement, de failles de sécurité. Ce caractère dual s'est encore manifesté lors de la crise de la covid : les solutions numériques ont permis de maintenir les emplois et l'éducation, tout en exposant particulièrement notre tissu économique aux cybermalveillances.

Ainsi, dans ma circonscription, les données numériques de la commune d'Erstein ont été dérobées à la suite d'une cyberattaque. C'est une véritable catastrophe puisque la commune a perdu tous ses contrats ainsi que son état civil. L'ouverture d'un fichier malveillant peut vraiment être lourde de conséquences.

Le groupe Agir ensemble considère que les risques numériques sont notamment issus de mauvaises pratiques résultant d'une pédagogie parfois inadaptée. En donnant aux consommateurs des informations plus lisibles pour répondre à ces risques numériques, perçus comme non tangibles ou difficiles à comprendre, la proposition de loi favorisera les changements d'usages et de comportements, ce qui poussera *in fine* les opérateurs à modifier leurs pratiques.

Cependant, le groupe estime qu'on aurait pu aller plus loin, notamment en donnant à l'ANSSI un pouvoir d'injonction. Ce serait une étape supplémentaire dans le développement de notre écosystème cyber et cela motiverait encore davantage ceux qui bénéficient de nos services.

Enfin, nous rejoignons M. Thierry Benoît dans l'idée que l'Europe est la bonne échelle pour réguler des opérateurs de taille mondiale. Nous ne manquerons pas d'encourager les initiatives qui pourraient être prises dans le cadre de la présidence française de l'Union européenne.

M. Christophe Naegelen, rapporteur. Monsieur Naillet, mon premier amendement devrait répondre à votre inquiétude puisqu'il vise à étendre la sécurisation aux sites internet, et non uniquement aux données personnelles et à celles des consommateurs.

Monsieur Latombe, s'agissant de votre amendement, avec lequel je suis en partie d'accord, nous aurons à discuter du niveau, législatif ou réglementaire, auquel devront être définis les critères de certification prenant en compte la localisation et la nationalité du propriétaire. Je pencherai pour une définition par l'ANSSI.

Monsieur Benoit, il est évident que la proposition de loi est la première pierre de la construction d'un mur, qui doit être européen, de protection des citoyens européens. La

présidence française devrait être non seulement le maître d'ouvrage, mais aussi le maçon de la construction de la sécurité numérique du quotidien.

Monsieur Herth, nous avons discuté de ce qui s'est passé dans une commune de votre circonscription. Les entreprises ne sont pas seules victimes des escroqueries et usurpations d'identité ; les collectivités le sont aussi, tout comme les particuliers. C'est pourquoi il faut agir rapidement et efficacement.

Madame Tiegna, je partage votre analyse et je vous remercie encore une fois pour notre travail commun.

La commission en vient à l'examen des articles.

Article 1er

Amendement CE5 de M. Christophe Naegelen et sous-amendement CE11 de M. Philippe Latombe.

M. Christophe Naegelen, rapporteur. Il s'agit de réécrire le dispositif proposé par le Sénat en l'élargissant. La sécurisation touchera non seulement les données personnelles, mais aussi les entreprises elles-mêmes. L'amendement définit également les entreprises concernées par la sécurisation, en y ajoutant les messageries.

M. Philippe Latombe. Les règles de cybersécurité varient selon que les données sont hébergées en Europe, en Russie, en Chine ou aux États-Unis. Par conséquent, le niveau de protection est totalement différent. L'ANSSI, dans son référentiel d'exigences applicables à un prestataire de services d'informatique en nuage pour l'obtention de la certification SecNumCloud, consacre une part importante de son travail à la localisation. C'est dans la loi que doit figurer cet élément essentiel, en application stricte du RGPD.

L'accord *Privacy shield*, couvrant le transfert de données personnelles entre l'Union européenne et les États-Unis, avait été conclu sur l'affirmation que le niveau de protection était équivalent de part et d'autre. La Cour de justice de l'Union européenne ayant invalidé cet accord, Facebook nous avait fait tout un sketch, prétendant qu'il serait obligé de quitter l'Europe. Cela montre à quel point la localisation des données est importante : loin d'être un sous-critère de la sécurisation, elle constitue un critère à part entière, qui doit donc relever de la loi, et non simplement du règlement.

Nous souhaitons, par ailleurs, renforcer l'éducation à la cybersécurité des consommateurs, qui doivent connaître exactement le niveau de cybersécurité des plateformes en ligne qu'ils visitent. La localisation des données personnelles est importante de ce point de vue, les consommateurs devant savoir où elles sont hébergées. Tel est l'objet de ce sous-amendement.

M. Christophe Naegelen, rapporteur. Lorsque nous avions auditionné l'ANSSI, j'avais eu le sentiment que ce n'était pas tant la localisation que la nationalité des propriétaires de l'endroit où sont hébergées les données qui importait. Je vous propose

donc de retirer votre sous-amendement afin de le retravailler en vue de la séance, en demandant son expertise à l'ANSSI.

M. Philippe Latombe. Ce point est très important pour nous. Je suis d'accord pour retirer mon sous-amendement et travailler à une rédaction qui puisse faire l'objet d'un amendement commun pour la séance. Un travail en concertation n'en aurait que plus de poids.

Mme Huguette Tiegna. Nous soutenons l'amendement du rapporteur. Il ne faut pas oublier qu'un décret viendra préciser certains aspects. Il faudra en tenir compte pour la nouvelle rédaction.

Le sous-amendement est ***retiré****.*

La commission ***adopte*** *l'amendement.*

En conséquence, l'amendement CE4 de M. Philippe Latombe ***tombe****.*

Amendement CE6 de M. Christophe Naegelen.

M. Christophe Naegelen, rapporteur. L'article adopté par le Sénat prévoit une autocertification, dont on ne peut guère envisager qu'elle lève les doutes que pourraient avoir nos concitoyens. Nous proposons de créer une véritable certification, délivrée par des organismes habilités par l'autorité administrative compétente, et qui ne laisse plus de place au doute.

La commission ***adopte*** *l'amendement.*

Elle ***adopte*** *successivement les amendements de cohérence CE7 et CE8 de M. Christophe Naegelen.*

Amendement CE9 de M. Christophe Naegelen.

M. Christophe Naegelen, rapporteur. Il s'agit, en quelque sorte, d'un amendement d'appel en ce sens qu'il énonce un but – la certification doit apparaître sur la première page qui s'ouvre à l'utilisateur, sans que celui-ci ait besoin d'aller la chercher –, en sachant que les modalités doivent être précisées avec les services.

La page d'accueil ou la connexion, envisagées dans un premier temps, ne sont pas toujours pertinentes. Ainsi, si vous cherchez une brosse à cheveux dans un moteur de recherche, vous serez envoyé directement sur la page de la brosse à cheveux et non sur la page d'accueil du site. C'est pourquoi il est nécessaire de faire apparaître cette mention sur la première page affichée.

Mme Huguette Tiegna. Cet amendement est très important et il ne faut pas rater la cible. Nous sommes d'accord sur le principe, mais il faut trouver la rédaction qui convient. Nous vous suggérons donc de retirer votre amendement en vue de la séance.

M. Philippe Latombe. Nous comprenons l'objectif de cet amendement, mais c'est sa déclinaison technique qui peut poser problème. Le diagnostic de cybersécurité doit-il apparaître à chacune des réponses à une recherche ou bien seulement sur la page vers laquelle envoie le lien fourni par le moteur de recherche lorsque l'on clique dessus ? Votre rédaction n'est pas suffisamment claire pour être efficace. Si j'étais rapporteur, je demanderais le retrait de l'amendement pour le retravailler en vue de la séance.

M. Christophe Naegelen, rapporteur. Compte tenu de la brièveté des délais, j'avais déposé cet amendement d'appel pour marquer le coup. Je vous propose d'y travailler ensemble, avec Mme Tiegna également, afin de déposer un amendement commun en séance.

L'amendement est ***retiré****.*

La commission ***adopte*** *l'article 1er* ***modifié****.*

Article 2 (supprimé)

La commission maintient la ***suppression*** *de l'article 2.*

Elle ***adopte*** *l'ensemble de la proposition de loi* ***modifiée****.*

LISTE DES PERSONNES AUDITIONNÉES

Audition commune :

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

M. Emmanuel Naegelen, directeur-adjoint

Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF)

Mme Nadine Mouy, sous-directrice des services, réseaux et numérique

M. Paul-Emmanuel Piel, chef de bureau des médias, communications électroniques, culturel, économie de la donnée

Pierre-Olivier Salles, adjoint au chef de bureau

Direction générale des entreprises (DGE)

M. Michel Rao, directeur de projet économie de la donnée et logiciel

Contribution écrite

MEDEF *

* *Ces représentants d'intérêts ont procédé à leur inscription sur le registre de la Haute Autorité pour la transparence de la vie publique, s'engageant ainsi dans une démarche de transparence et de respect du code de conduite établi par le Bureau de l'Assemblée nationale.*