ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 43236	De **M. Christophe Naegelen** (UDI et Indépendants - Vosges)	**Question écrite**

Ministère interrogé > Transition numérique et communications électroniques	**Ministère attributaire** > Transition numérique et communications électroniques

Rubrique >numérique	**Tête d'analyse** >Cybersécurité et Digital Markets Act	**Analyse** > Cybersécurité et Digital Markets Act.

Question publiée au JO le : **21/12/2021**
Réponse publiée au JO le : **15/02/2022** page : **1053**

Texte de la question

M. Christophe Naegelen interroge M. le secrétaire d'État auprès des ministres de l'économie, des finances et de la relance, et de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques sur l'articulation entre la législation française et la législation européenne en matière de cybersécurité. Dans la continuité d'une trajectoire initiée en 2019, le nombre de victimes de cyberattaques en France a été multiplié par quatre en 2020, d'après l'Autorité nationale de la sécurité des systèmes d'information (ANSSI). Cette situation est particulièrement préoccupante, notamment dans un contexte de numérisation croissante et de recours régulier à des services à distance, où toute cyberattaque est, de fait, susceptible d'avoir un impact accru. La cybersécurité est par conséquent un enjeu majeur qui appelle une réponse des pouvoirs publics adaptée afin que demain, chaque utilisateur soit conscient des risques qu'engendrent ces usages et qu'il s'en prémunisse au maximum. Adoptée en première lecture par le Parlement, la proposition de loi pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public poursuit cet objectif. Elle devrait permettre de renforcer l'information du grand public quant à la sécurisation de certaines plateformes et de certains services numériques. L'audit de cybersécurité prévu par ce texte constituera un facteur de confiance qui sera, demain, déterminant pour les entreprises qui fournissent ces services de communication au public. Afin de garantir la pleine efficacité de cet audit dans le temps long, il convient néanmoins de prendre en considération les nouvelles régulations des marchés numériques en cours de discussion au niveau européen et d'anticiper les enjeux de cybersécurité afférents. En effet, la future mise en œuvre du projet de règlement *Digital Markets Act* amènera des évolutions profondes de certains de ces services, dont les conséquences auraient, dans certains cas, pour effet indésirable l'augmentation du potentiel de menaces. À titre d'exemple, les effets sur l'augmentation de la fraude et des cyberattaques du chargement latéral, dit « *sideloading* », mesure unanimement déconseillée par l'ENISA et l'ensemble des agences européennes de cybersécurité mais qui sera, demain, une obligation à respecter par les opérateurs en vertu du *Digital Markets Act*, ne doivent pas être négligés. Le nouveau cadre de régulation de la concurrence des marchés numériques ambitionné par les co-législateurs européens ne doit pas, demain, priver ces acteurs de leur capacité à répondre pleinement à l'objectif poursuivi par le Parlement à travers cette proposition de loi : celui de garantir la cybersécurité des concitoyens. En conséquence, il lui demande comment le Gouvernement entend concilier ces deux objectifs.

Texte de la réponse

Le Digital Markets Act (« DMA ») vise à interdire a priori les pratiques anti-concurrentielles les plus délétères des

géants du numérique et à équilibrer les relations entre les plateformes qui contrôlent l'accès à certains marchés (« gatekeepers ») et les entreprises qui proposent leurs offres sur ceux-ci. L'obligation 6 (c) du DMA permettra effectivement aux utilisateurs d'installer, sur les systèmes d'exploitation (OS) des gatekeepers, d'autres magasins d'applications que ceux qui sont contrôlés par ces acteurs ; ainsi que de télécharger des applications directement sur internet, sans passer par un magasin d'applications. Cette obligation se fera au profit : des entreprises (en particulier les développeurs d'applications) qui seront libres de proposer leurs services, sans se voir imposer des pratiques tarifaires inéquitables ou des politiques éditoriales, et des consommateurs qui auront plus de choix de services et pourront davantage paramétrer leurs terminaux. Afin de garantir la cybersécurité des concitoyens, cette obligation prévoit « une clause de sauvegarde » qui permet aux gatekeepers de prendre les mesures qui sont nécessaires et proportionnées pour : éviter que les applications et magasins d'applications tiers ne compromettent l'intégrité du terminal ou de l'OS fourni par le gatekeeper; et que les utilisateurs puissent assurer leur sécurité vis-à-vis des applications et magasins d'applications tiers téléchargés sur l'OS du gatekeeper. En effet, la majorité des éléments qui assurent la sécurité des utilisateurs sont construits directement sur l'OS et/ou le terminal ou alors ne sont pas spécifiques à un magasin d'application exclusif (par exemple, un examen humain des applications peut s'effectuer quel que soit le magasin d'applications). En outre, il n'existe aucune raison pour que les magasins d'applications tiers ne soient pas en mesure de se conformer aux exigences techniques destinées à assurer la sécurité de l'appareil, sachant que les gatekeepers font déjà appel à des fournisseurs tiers pour certains services qui fonctionnent sur leurs OS (par exemple, Apple fait appel à des services de paiement tiers pour traiter les paiements in-app effectués sur son App Store). Ainsi, le DMA n'empêche pas aux magasins d'applications alternatifs d'offrir un niveau de protection comparable à celui proposé par les gatekeepers. Par ailleurs, la cybersécurité des utilisateurs peut également être assurée lorsque les utilisateurs ont la possibilité de télécharger des applications directement sur internet puisque des processus existent pour auditer les applications et protéger le matériel informatique de tout contenu malveillant (exemple du processus de « notarization » via le système Gatekeeper utilisé par Apple sur ses ordinateurs qui fonctionnent sur Mac OS). Un système similaire pourrait être utilisé pour assurer la sécurité, tout en autorisant des canaux de distribution alternatifs : soit directement au niveau des applications (en fournissant des certificats de confiance directement aux éditeurs concernés), soit au niveau de magasins d'applications tiers pour garantir leur niveau de sécurité au vue d'une liste objective d'exigences de vérifications et d'engagements de responsabilité. Pour conclure, le DMA prévoit des obligations fortes pour ouvrir les écosystèmes des gatekeepers, sans pour autant négliger la sécurité des utilisateurs et des systèmes. Les objectifs du DMA n'entendent donc pas remettre en cause ceux de la proposition de loi pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public.