ASSEMBLÉE NATIONALE

22 novembre 2021

POUR LA MISE EN PLACE D'UNE CERTIFICATION DE CYBERSÉCURITÉ DES PLATEFORMES NUMÉRIQUES DESTINÉE AU GRAND PUBLIC - (N° 4700)

Commission	
Gouvernement	

Non soutenu

AMENDEMENT

N º 1 (Rect)

présenté par
Mme Forteza, Mme Bagarry, Mme Batho, Mme Gaillot, M. Orphelin et M. Villani

---

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 2, insérer l'article suivant:

L’article 323-1 du code pénal est complété par un alinéa ainsi rédigé :

« Ne peut donner lieu à des poursuites pénales le délit prévu au premier alinéa, commis par une personne de bonne foi qui transmet, à la seule autorité nationale de sécurité des systèmes d’information, une information sur l’existence d’une vulnérabilité concernant la sécurité d’un système de traitement automatisé de données. »

EXPOSÉ SOMMAIRE

Alors que les annonces de failles informatiques se succèdent quotidiennement, touchant tous types d’acteurs, cet amendement vise à améliorer la protection accordée aux lanceurs d’alerte de sécurité informatique.

En 2016, à l’occasion de l’examen du projet de loi pour une République numérique, le législateur a effectué un premier pas en permettant aux « white hats », ou « hackers éthiques », de signaler des failles auprès de l’Agence nationale de sécurité des systèmes d'information (ANSSI), avec différentes garanties de confidentialité, notamment quant à leur identité.

De plus, en dérogation aux obligations posées par l’article 40 du code de procédure pénale, l’ANSSI n’est pas tenue de dénoncer d’éventuels faits constitutifs du délit prévu à l’article L 323-1 du code pénal. Ses dispositions punissent de deux ans d’emprisonnement et 60 000 euros d’amende « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* ».

Afin d’encourager la révélation de failles – et, par la suite, leur correction –, ceci au nom de l’intérêt général, cet amendement propose de franchir une étape supplémentaire en prévoyant une exemption de poursuites au titre du délit prévu à l’article L 323-1 précité, pour toutes les personnes qui, de bonne foi, transmettent à l’ANSSI des informations sur l'existence de vulnérabilités concernant la sécurité de systèmes de traitement automatisé de données.

Cette proposition rejoint pleinement les recommandations du rapport « *Améliorer la protection des lanceurs d’alerte partout en Europe* » du Conseil de l'Europe du 1er octobre 2019, au sein duquel le rapporteur du texte, Sylvain Waserman, suggère que la criminalisation de l'accès à un système de données soit limitée « *aux « effractions » informatiques commises à des fins de gains personnels, sans aucun lien avec le signalement d’informations dans l’intérêt public* ».

Cet amendement a été travaillé avec l’association La Maison des lanceurs d’alerte.