ASSEMBLÉE NATIONALE

15 janvier 2018

ADAPTATION AU DROIT DE L'UE DANS LE DOMAINE DE LA SÉCURITÉ - (N° 530)

Rejeté

AMENDEMENT

N º CL9

présenté par
Mme Obono, Mme Autain, M. Bernalicis, M. Coquerel, M. Corbière, Mme Fiat, M. Lachaud, M. Larive, M. Mélenchon, Mme Panot, M. Prud'homme, M. Quatennens, M. Ratenon, Mme Ressiguier, Mme Rubin, M. Ruffin et Mme Taurine

---

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 15, insérer l'article suivant:

Le chapitre Ier du titre II du livre III de la deuxième partie du code de la défense est complété par un article L. 2321-5 ainsi rédigé :

« I. – Pour les besoins de la sécurité des systèmes d'information, les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 peuvent organiser des programmes dits de "primes de bug" pour lesquels ils peuvent notamment proposer des primes.

« II. – Seuls peuvent participer aux programmes mentionnés au I les personnes physiques qui ont été dûment enregistrées en tant que "chasseur de failles informatiques", auprès de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1. Cet enregistrement fait l'objet d'une procédure qui est précisée par décret en Conseil d'État. L'agence peut toujours, pour des raisons impérieuses d'intérêt général, refuser ou retirer cet enregistrement, par décision motivée et précédée d'une procédure contradictoire dans les conditions prévues au chapitre II du titre II du livre Ier du code des relations entre le public et l'administration. »

EXPOSÉ SOMMAIRE

Par cet amendement, nous souhaitons utilement soutenir les efforts de renforcement de la cybersécurité en France.

En effet, ce alors même que l'informatique est devenue structurante dans et pour le fonctionnement de nombreux services publics, administrations, entreprises, associations, les vulnérabilités de sécurité informatique sont devenues d'autant plus nombreuses.

S'est ainsi développée une activité pouvant être à la fois lucrative et non lucrative, celle des « découvreurs de failles », ou « chasseurs de vulnérabilités de sécurité ». En effet, un « bug

bounty » (ou « prime » de dysfonctionnement) est une récompense qu'une entreprise peut offrir à tous ceux qui trouvent des failles de sécurité dans un périmètre donné.

Nous sommes conscients de l’importance de ces « bug bounty » et de ce travail de fond des « découvreurs de failles », puisque contrairement aux interventions ponctuelles de sociétés en conseil informatique extérieures, les « bug bounty » permettent une amélioration continue contre des attaques ou tentatives d’attaques qui se renouvellement quasi quotidiennement, tant dans leurs méthodes que dans leur ampleur.

A cet effet, nous proposons ici, par cet amendement d'appel, d'envisager la création d'un statut juridique des "chasseurs de faille", qui puisse permettre juridiquement l'organisation de "bug bounty", ce pour l'instant dans le périmètre restreint des opérateurs considérés comme essentiels par le code de la défense / que nous souhaitons voir à terme étendu bien sûr à l'économie en général.

En prévoyant ici que pour ce premier statut juridique du "chasseur de faille", celui-ci soit enregistré - autorisé - par l'ANSSI (Agence nationale de sécurité des systèmes d'information), le "chasseur de failles" pourra disposer d'une protection (et ne pas se voir directement menacé d'être accusé de piratage informatique / d'être dans l'illégalité). Ceci permettrait en outre de faire basculer du bon côté un grand nombre de spécialistes informatiques qui restent dans une zone oscillant entre la légalité et l'illégalité (dénommés "grey hats" en référence aux "blancs / white : spécialistes éthiques et "black / noirs" : spécialistes dans l'ombre et dans l'illégalité).

Cet amendement va de pair avec un autre de nos amendements, qui lui est un amendement d'appel demandant une étude spécifique sur cette question.