

ASSEMBLÉE NATIONALE

15 janvier 2018

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

Rejeté

AMENDEMENT

N° CL10

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 Gouvernement remet au Parlement, dans un délai de six mois à compter de la promulgation de la présente loi, un rapport proposant la création d'un statut juridique spécifique pour les "chasseurs de failles informatiques" et les programmes dits de "prime de bug" ou "bug bounty", afin de promouvoir la cybersécurité informatique par amélioration continue et encourager la contribution de ces mêmes spécialistes informatiques. »

EXPOSÉ SOMMAIRE

Par cet amendement, nous souhaitons utilement soutenir les efforts de renforcement de notre cybersécurité.

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.

C'est ainsi développé 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 renouvellent quasi quotidiennement, tant dans leurs méthodes que dans leur ampleur.

A cet effet, nous proposons ici qu'un rapport puisse permettre la création d'un statut juridique des "chasseurs de faille", qui puisse permettre qu'hors des séquences de "bug bounty" organisés par une entreprise elle-même, ou un organisme lui-même, le "chasseur de faille" 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 amendement, qui lui est un amendement d'appel et législatif sur cette question.