

ASSEMBLÉE NATIONALE

16 septembre 2016

TRANSPARENCE, LUTTE CONTRE LA CORRUPTION ET MODERNISATION DE LA VIE
ÉCONOMIQUE - (N° 3939)

Non soutenu

AMENDEMENT

N° CL39

présenté par
Mme Kosciusko-Morizet

ARTICLE 6 B

I. - Compléter cet article par l'alinéa suivant :

« II. - Le premier alinéa de l'article 323-1 du code pénal est complété par une phrase ainsi rédigée :
« Toute personne qui a tenté de commettre ou commis ce délit de bonne foi est exemptée de poursuites si, ayant averti immédiatement l'autorité administrative ou judiciaire, ou le responsable du système de traitement automatisé de données en cause, elle a permis d'éviter toute atteinte ultérieure aux données ou au fonctionnement du système ».

II. - En conséquence, au début de l'alinéa 1, insérer la référence : « I. - ».

EXPOSÉ SOMMAIRE

Le présent amendement a pour objet de protéger les lanceurs d'alerte de sécurité informatique.

Certaines personnes, lorsqu'elles découvrent de bonne foi une faille sur un site web, avertissent le responsable de ce site afin de permettre la résolution du problème et la protection des données mises en danger. Elles jouent ainsi un rôle utile de lanceurs d'alerte.

Or, selon le code pénal, tout accès non autorisé à un système peut être considéré comme frauduleux (articles 323-1 alinéa 1). Le simple fait de vérifier l'existence d'une faille constitue un accès non autorisé, donc une infraction.

Dans la jurisprudence Kitetoa (2002), un journaliste qui avait trouvé des données clients en accès libre sur le site du groupe Tati, avait prévenu ce dernier d'une faille sur son site web. Tati l'avait néanmoins attaqué en justice pour accès frauduleux à son système d'information. Après avoir été condamné en première instance, le journaliste avait finalement été relaxé en appel, au motif que puisque les données étaient librement accessibles par un simple navigateur web, et n'étaient pas indiquées comme n'étant pas publiques, on ne pouvait pas sanctionner le fait d'y accéder.

L'arrêt du 9 septembre 2009 de la cour d'appel de Paris, statuant en référé dans l'affaire Zataz, apporte un point de vue différent. Dans une affaire a priori similaire, la Cour énonce que l'accès non autorisé à un système constitue un « trouble manifestement illicite », et le journaliste qui avait signalé la faille de sécurité dans le système de la société FLP s'est vu ordonner de rendre inaccessible son article et de détruire les pièces copiées sur le serveur, tout en étant condamné aux dépens.

Enfin, dans l'affaire Bluetouff, la Cour de cassation vient de rejeter en mai 2015 le pourvoi d'un blogueur condamné à 3000 € d'amende pour avoir téléchargé des fichiers sur le site d'une agence de sécurité sanitaire, fichiers qui étaient pourtant en accès libre du fait d'un défaut de sécurisation du site.

Le risque est désormais de dissuader ceux qui découvrent des failles de les signaler aux responsables informatiques, par peur de poursuites judiciaires. Sans lanceurs d'alerte, les sites mal protégés resteraient alors plus longtemps vulnérables face à des internautes mal intentionnés.

Afin de permettre aux internautes de continuer à exercer leur vigilance sur les failles de sécurité, jouant ainsi le rôle utile de sentinelles du web, et afin d'éviter la répétition de jurisprudences contradictoires et incertaines, il serait souhaitable d'établir un cadre juridique exonérant de responsabilité les lanceurs d'alerte, personnes détectant et signalant les failles de sécurité informatique de bonne foi, sans intention de nuire, par exemple en s'inspirant de l'article 221-5-3 du code pénal qui dispose pour les assassinats : « Toute personne qui a tenté de commettre les crimes d'assassinat ou d'empoisonnement est exempte de peine si, ayant averti l'autorité administrative ou judiciaire, elle a permis d'éviter la mort de la victime et d'identifier, le cas échéant, les autres auteurs ou complices ».

Cet amendement avait déjà été proposé dans le cadre du projet de loi pour une République numérique. Contrairement à ce qui a pu être dit lors des débats, son adoption ne permettrait aucunement à un hacker malveillant de rechercher l'impunité en envoyant un avertissement *après* avoir commis des actes hostiles contre le système d'information ou après avoir volé des informations. En effet, l'amendement proposé ne couvre que l'accès au système ; les éventuelles modifications, altérations, soustractions d'informations, introductions frauduleuses de données ou de virus, attaques en déni de service... constituent des infractions distinctes, réprimées par d'autres articles du Code pénal (principalement 323-2 et suivants) et ne sont pas concernées par le présent amendement.

Les rédactions alternatives proposées lors des débats sur le projet de loi pour une République numérique ne sont pas non plus satisfaisantes : en exemptant de peine mais pas de poursuite (rédaction de l'Assemblée nationale), ou en se contentant d'autoriser à l'ANSSI à ne pas poursuivre systématiquement le lanceur d'alerte (rédaction du Sénat et de la Commission mixte paritaire), ces dispositions n'apportent pas une véritable sécurité à ce dernier, qui risque toujours des poursuites (même s'il n'y a pas de peine à la fin) et qui devra assumer le coût de sa défense.

Pour ces raisons, cet amendement est à nouveau proposé.