

Le hacking légal et rémunéré, vous connaissez ?

 <p>Denis JACOPINI EXPERT JUDICIAIRE vous informe</p>	<p>Le hacking légal et rémunéré, vous connaissez ?</p>
--	--

Le hacking : « accès et maintien frauduleux dans un système de traitement automatisé de données » va changer. Le 21 janvier 2016, l'Assemblée nationale a adopté, en première lecture, un amendement contenu dans le projet de loi pour une République numérique visant à compléter l'article 323-1 du Code pénal, par un nouvel alinéa :

« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système ».

Cet amendement, nommé « Bluetouff » en référence à l'arrêt de la Cour de cassation du 20 mai 2015 qui avait condamné un internaute pour s'être maintenu frauduleusement dans l'intranet de l'ANSES, prévoit, comme en matière d'association de malfaiteurs, une exemption de peine pour toute personne qui, après avoir constaté, voire exploité, une faille de sécurité en informe immédiatement l'autorité publique ou le maître du système.

Il ne s'agit là que d'une exemption de peine, et non d'une exemption de poursuites, ce qui en d'autres termes signifie que l'auteur du hacking, du piratage pourra être poursuivi et déclaré coupable, mais n'aura pas à exécuter de peines pénales.

Par cet amendement, le Gouvernement entend poursuivre un double objectif. D'abord donner une alternative presque légale au hacker du dimanche qui par défi personnel, et non intention de nuire, est parvenu à s'introduire dans un système d'information. A ce titre, il est regrettable que l'amendement Bluetouff ne prévoit qu'une exemption de peine, l'assurance de ne pas être poursuivi pour hacking aurait, à n'en pas douter, été plus convaincante.

En second lieu, il permettrait de participer à la sécurité du réseau. Garantie en poche de ne pas être pénalisés, nombre d'experts en informatique pourraient collaborer avec les sociétés développant des sites internet, applications ou logiciels pour identifier et corriger les vulnérabilités.

Ce dispositif serait, toutefois, incomplet s'il ne pouvait, par ailleurs, s'appuyer sur des initiatives de plus en plus courantes du secteur privé.

Les grands noms de l'internet et de l'informatique sont de plus en plus nombreux à proposer, souvent contre rémunération, aux hackers bien intentionnés de collaborer avec eux pour détecter les failles de sécurité.

Calqué sur ce qui existe déjà aux Etats-Unis avec la plateforme HackerOne, le site européen Bounty Factory mettant en relation hackers et entreprises du net permet depuis peu, en échange de récompenses pour toute faille décelée et corrigée, de signaler en ligne les vulnérabilités.

Législateur et secteur privé s'acheminent progressivement vers un droit au hacking. En attendant, le Code pénal nous rappelle qu'« accéder ou se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende ».

Virginie Bensoussan-Brulé

Julien Kahn

Lexing Pénal numérique

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

Réagissez à cet article

Source : *Le hacking ça peut payer... légalement*